PGP® Desktop für Mac OS X

Benutzerhandbuch

Versionsinformationen

PGP Desktop für Macintosh OS X Benutzerhandbuch. PGP Desktop Version 10.1.2. Veröffentlicht am März 2011

Copyright-Informationen

Copyright © 2011, PGP Corporation. Alle Rechte vorbehalten. Dieses Dokument darf ohne ausdrückliche schriftliche Genehmigung der PGP Corporation weder im Ganzen noch in Teilen, in keiner Form und auf keine Weise, weder mechanisch noch elektronisch und zu keinem Zweck vervielfältigt oder weitergegeben werden.

Markeninformationen

PGP, Pretty Good Privacy und das PGP-Logo sind in den USA und anderen Ländern eingetragene Marken der PGP Corporation. IDEA ist eine Marke der Ascom Tech AG. Windows und ActiveX sind eingetragene Marken der Microsoft Corporation. AOL ist eine eingetragene Marke und AOL Instant Messenger ist eine Marke von America Online, Inc. Red Hat und Red Hat Linux sind Marken oder eingetragene Marken von Red Hat, Inc. Linux ist eine eingetragene Marke von Linus Torvalds. Solaris ist eine Marke oder eingetragene Marke von Sun Microsystems, Inc. AIX ist eine Marke oder eingetragene Marke von International Business Machines Corporation. HP-UX ist eine Marke oder eingetragene Marke der Hewlett-Packard Company. SSH und Secure Shell sind Marken von SSH Communications Security, Inc. Rendezvous und Mac OS X sind Marken oder eingetragene Marken von Apple Computer, Inc. Alle anderen eingetragenen und nicht eingetragenen Marken, die in diesem Dokument erwähnt werden, sind alleiniges Eigentum ihrer jeweiligen Inhaber.

Lizenzierungs- und Patentinformationen

Der IDEA-Kryptografiealgorithmus, der in US-Patent Nr. 5.214.703 beschrieben wird, wurde von der Ascom Tech AG lizenziert. Der Verschlüsselungsalgorithmus CAST-128, der im RFC 2144 beschrieben wird, ist weltweit für kommerzielle und nicht kommerzielle Zwecke ohne Lizenzgebühren freigegeben. Die PGP Corporation hat sich eine Lizenz auf die Patentrechte im Patentantrag des Aufsichtskomitees der University of California mit der Seriennummer 10/655.563 und dem Titel „Block Cipher Mode of Operation for Constructing a Wide-blocksize block Cipher from a Conventional Block Cipher" gesichert. Teile der Software von Drittanbietern, die in PGP Universal Server enthalten sind, sind gemäß der GNU General Public License (GPL) lizenziert. PGP Universal Server als Ganzes ist nicht gemäß der GPL lizenziert. Wenn Sie eine Kopie des Quellcodes der in PGP Universal Server enthaltenen GPL-Software anfordern möchten, wenden Sie sich an den *PGP-Support* (*https://support.pgp.com*). Die PGP Corporation verfügt möglicherweise über Patente und/oder zum Patent angemeldete Anwendungen für Inhalte dieser Software oder ihrer Dokumentation. Mit der Bereitstellung dieser Software oder Dokumentation werden Ihnen keine Lizenzrechte für besagte Patente übertragen.

Danksagungen

Dieses Produkt kann Folgendes enthalten:

– Die von Mark Adler und Jean-Loup Gailly erstellten Komprimierungscodes Zip und ZLib werden mit Genehmigung der kostenlosen Info-ZIP-Implementierung verwendet, die von zlib (http://www.zlib.net) entwickelt wurde. – Libxml2, den XML C-Parser und das XML C-Toolkit, die für das Gnome-Projekt entwickelt wurden und gemäß der MIT-Lizenz (http://www.opensource.org/licenses/mit-license.html) vertrieben werden und urheberrechtlich geschützt sind. Copyright © 2007, Open Source Initiative. – bzip2 1.0, eine kostenlos verfügbare hochwertige Datenkomprimierungsanwendung, urheberrechtlich geschützt durch Julian Seward, © 1996-2005. – Anwendungsserver (http://jakarta.apache.org/), Webserver (http://www.apache.org/), Jakarta Commons (http://jakarta.apache.org/commons/license.html) und log4j, eine auf Java basierende Bibliothek für die Analyse von HTML, entwickelt von der Apache Software Foundation. Die Lizenz ist unter www.apache.org/licenses/LICENSE-2.0.txt verfügbar. – Castor, ein auf Open Source basierendes Datenbindungs-Framework zum Übertragen von Daten aus XML in Java-Objekte und aus Java in Datenbanken, wird von der ExoLab Group gemäß einer Apache 2.0-ähnlichen Lizenz veröffentlicht, die unter http://www.castor.org/license.html verfügbar ist. – Xalan, eine Open-Source-Softwarebibliothek der Apache Software Foundation, die die XML-Transformationssprache XSLT und die XML-Abfragesprache XPath implementiert, wird gemäß der Apache Software-Lizenz Version 1.1 veröffentlicht, die unter http://xml.apache.org/xalan-j/#license1.1 verfügbar ist. – Apache Axis, eine Implementierung von SOAP (Simple Object Access Protocol), die für Kommunikationen zwischen verschiedenen PGP-Produkten verwendet wird, wird gemäß der Apache-Lizenz bereitgestellt, die unter http://www.apache.org/licenses/LICENSE-2.0.txt verfügbar ist. – mx4j, eine Open-Source-Implementierung der Java Management Extensions (JMX), wird gemäß einer Apache-ähnlichen Lizenz veröffentlicht, die unter http://mx4j.sourceforge.net/docs/ch01s06.html verfügbar ist. – jpeglib Version 6a basiert teilweise auf den Arbeiten der Independent JPEG Group (http://www.ijg.org/). – libxslt, eine XSLT C-Bibliothek, die für das GNOME-Projekt entwickelt wurde und für XML-Transformationen verwendet wird, wird gemäß der MIT-Lizenz (http://www.opensource.org/licenses/mit-license.html) vertrieben. – PCRE-Perl-Compiler für reguläre Ausdrücke, urheberrechtlich geschützt und vertrieben von der University of Cambridge. ©1997-2006. Das Lizenzabkommen ist unter http://www.pcre.org/license.txt verfügbar. – BIND-Protokolle für Balanced Binary Tree Library und Domain Name System (DNS), von Internet Systems Consortium, Inc. (http://www.isc.org) entwickelt und urheberrechtlich geschützt. – Kostenlose BSD-Implementierung von Daemon, entwickelt von The FreeBSD Project, © 1994-2006. – Simple Network Management Protocol Library, entwickelt und urheberrechtlich geschützt von der Carnegie Mellon University © 1989, 1991, 1992, Networks Associates Technology, Inc, © 2001-2003, Cambridge Broadband Ltd. © 2001-2003, Sun Microsystems, Inc., © 2003, Sparta, Inc, © 2003-2006, Cisco, Inc. und Information Network Center of Beijing University of Posts and Telecommunications, © 2004. Das Lizenzabkommen hierfür ist unter http://net-snmp.sourceforge.net/about/license.html verfügbar. – NTP Version 4.2, entwickelt von Network Time Protocol und von mehreren Beitragenden urheberrechtlich geschützt. – Lightweight Directory Access Protocol, entwickelt und urheberrechtlich geschützt von der OpenLDAP Foundation. OpenLDAP ist eine Open-Source-Implementierung des Lightweight Directory Access Protocol (LDAP). Copyright © 1999-2003, The OpenLDAP Foundation. Das Lizenzabkommen ist unter http://www.openldap.org/software/release/license.html verfügbar. Secure Shell OpenSSH, entwickelt und veröffentlicht vom OpenBSD Project gemäß einer BSD-ähnlichen Lizenz, die unter http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/LICENCE?rev=HEAD verfügbar ist. – PC/SC Lite ist eine kostenlose Implementierung von PC/SC, einer Spezifikation für die Integration von Smartcards, die gemäß der BSD-Lizenz veröffentlicht wird. – Postfix, ein Mail Transfer Agent (MTA) auf Open-Source-Basis, wird gemäß der IBM Public License 1.0 veröffentlicht, die unter http://www.opensource.org/licenses/ibmpl.php verfügbar ist. – PostgreSQL, ein kostenloses objektrelationales Datenbankverwaltungssystem, wird gemäß einer BSD-ähnlichen Lizenz veröffentlicht, die unter http://www.postgresql.org/about/licence verfügbar ist. – PostgreSQL-JDBC-Treiber, ein kostenloses Java-Programm zum Herstellen einer Verbindung mit PostgreSQL-Datenbanken über standardmäßigen, datenbankunabhängigen Java-Code, (c) 1997-2005, PostgreSQL Global Development Group, wird gemäß einer BSD-ähnlichen Lizenz veröffentlicht, die unter http://jdbc.postgresql.org/license.html verfügbar ist. – PostgreSQL Regular Expression Library, ein kostenloses objektrelationales Datenbankverwaltungssystem, wird gemäß einer BSD-ähnlichen Lizenz veröffentlicht, die unter http://www.postgresql.org/about/licence verfügbar ist. – 21.vixie-cron ist die Vixie-Version von cron, einem UNIX-Standarddaemon, der bestimmte Programme zu vorgegebenen Zeiten ausführt. Copyright © 1993, 1994, Paul Vixie; mit Genehmigung verwendet. – JacORB, ein Java-Objekt, das zur Verbesserung der Kommunikation zwischen in Java geschriebenen Prozessen und der Datenschicht verwendet wird, wird als Open Source gemäß der GNU Library General Public License (LGPL) lizenziert, die unter http://www.jacorb.org/lgpl.html verfügbar ist. Copyright © 2006 The JacORB Project. – TAO (The ACE ORB) ist eine Open-Source-

Implementierung eines CORBA Object Request Broker (ORB) und wird zur Kommunikation zwischen in C/C++ geschriebenen Prozessen und der Datenschicht verwendet. Copyright (c) 1993-2006, Douglas C. Schmidt und seine Forschungsgruppe an der Washington University, der University of California, Irvine und der Vanderbilt University. Die Open-Source-Softwarelizenz ist unter http://www.cs.wustl.edu/~schmidt/ACE-copying.html verfügbar. – libcURL, eine Bibliothek zum Herunterladen von Dateien über gemeinsame Netzwerkdienste, ist eine Open-Source-Software, die gemäß einer Ableitung der MIT/X-Lizenz bereitgestellt wird, die unter http://curl.haxx.se/docs/copyright.html verfügbar ist. Copyright (c) 1996-2007, Daniel Stenberg. – libuuid, eine Bibliothek zur Erstellung eindeutiger Bezeichner, wird gemäß einer BSD-ähnlichen Lizenz veröffentlicht, die unter http://thunk.org/hg/e2fsprogs/?file/fe55db3e508c/lib/uuid/COPYING verfügbar ist. Copyright (C) 1996, 1997 Theodore Ts'o. – libpopt, eine Bibliothek zum Analysieren von Befehlszeilenoptionen, wird gemäß den Bestimmungen der GNU Free Documentation License veröffentlicht, die unter http://directory.fsf.org/libs/COPYING.DOC verfügbar ist. Copyright © 2000-2003 Free Software Foundation, Inc. – gSOAP, ein Entwicklungstool für Windows-Clients für die Kommunikation mit dem AMT-Chipsatz der Intel Corporation auf der Hauptplatine, wird gemäß der gSOAP Public License, Version 1.3b, bereitgestellt, die unter http://www.cs.fsu.edu/~engelen/license.html verfügbar ist. – Die Windows Template Library (WTL) wird zur Entwicklung von Komponenten der Benutzeroberfläche verwendet und gemäß der Common Public License v1.0 bereitgestellt, die unter http://opensource.org/licenses/cpl1.0.php verfügbar ist. – Das Perl-Kit umfasst mehrere unabhängige Dienstprogramme für die Automatisierung verschiedener Verwaltungsfunktionen und wird gemäß der Perl Artistic License bereitgestellt, die unter http://www.perl.com/pub/a/language/misc/Artistic.html verfügbar ist. – rEFIt - libeg stellt eine graphische Schnittstellenbibliothek für EFI bereit, einschließlich Bild- und Textwiedergabe sowie Alpha-Blending, und wird gemäß der Lizenz bereitgestellt, die unter http://refit.svn.sourceforge.net/viewvc/*checkout*/refit/trunk/refit/LICENSE.txt?revision=288 verfügbar ist. Copyright (c) 2006 Christoph Pfisterer. Alle Rechte vorbehalten. – Java Radius Client für die Authentifizierung von PGP Universal Web Messenger-Benutzern über Radius wird gemäß der Lesser General Public License (LGPL) bereitgestellt, die unter http://www.gnu.org/licenses/lgpl.html verfügbar ist. – Yahoo! User Interface (YUI)-Bibliothek, Version 2.5.2, eine Webbenutzeroberflächen-Schnittstellenbibliothek für AJAX. Copyright (c) 2009, Yahoo! Inc. Alle Rechte vorbehalten. Veröffentlicht gemäß einer BSD-ähnlichen Lizenz, die unter http://developer.yahoo.com/yui/license.html verfügbar ist. – JSON-lib, Version 2.2.1, eine Java-Bibliothek, die zum Konvertieren von Java-Objekten in JSON-Objekte (JavaScript Object Notation) für AJAX verwendet wird. Bereitgestellt gemäß der Apache 2.0-Lizenz, die unter http://json-lib.sourceforge.net/license.html verfügbar ist. – EZMorph, verwendet von JSON-lib, wird gemäß der Apache 2.0-Lizenz bereitgestellt, die unter http://ezmorph.sourceforge.net/license.html verfügbar ist. – Apache Commons Lang, verwendet von JSON-lib, wird gemäß der Apache 2.0-Lizenz bereitgestellt, die unter http://commons.apache.org/license.html verfügbar ist. – Apache Commons BeanUtils, verwendet von JSON-lib, wird gemäß der Apache 2.0-Lizenz bereitgestellt, die unter http://commons.apache.org/license.html verfügbar ist. – SimpleIni ist ein Dateiparser im INI-Format und ermöglicht das Lesen und Schreiben von INI-Dateien, einem gängigen, von Windows verwendeten Format für Konfigurationsdateien, auf anderen Plattformen. Bereitgestellt gemäß der MIT-Lizenz, die unter http://www.opensource.org/licenses/mit-license.html verfügbar ist. Copyright 2006-2008, Brodie Thiesfield. – uSTL bietet eine kleine und schnelle Implementierung gängiger Funktionen und Datenstrukturen der Standard Template Library und wird gemäß der MIT-Lizenz bereitgestellt, die unter http://www.opensource.org/licenses/mit-license.html verfügbar ist. Copyright (c) 2005-2009, Mike Sharov <msharov@users.sourceforge.net>. – Protocol Buffers (protobuf), das Datenaustauschformat von Google, werden für die Serialisierung von Strukturdaten im PGP-SDK verwendet. Bereitgestellt gemäß der BSD-Lizenz, die unter http://www.opensource.org/licenses/bsd-license.php verfügbar ist. Copyright 2008 Google Inc. Alle Rechte vorbehalten.

Weitere Danksagungen und rechtliche Hinweise sind als Teil des PGP Universal Server enthalten.

Exportinformationen

Der Export dieser Software und ihrer Dokumentation unterliegt u. U. den entsprechenden Durchführungsbestimmungen des Bureau of Export Administration, United States Department of Commerce, die den Export und Reexport von bestimmten Produkten und technischen Daten einschränken.

Nutzungseinschränkungen

Die Software, zu der diese Dokumentation gehört, wird Ihnen für die persönliche Nutzung zu den Bedingungen lizenziert, die im mit der Software gelieferten Endbenutzerlizenzabkommen (EULA) aufgeführt sind. Die Informationen in diesem Dokument können ohne Vorankündigung geändert werden. Die PGP Corporation garantiert nicht, dass die Informationen Ihre Anforderungen erfüllen oder dass sie fehlerfrei sind. Die Informationen können technische Ungenauigkeiten oder Tippfehler enthalten. Diese Informationen können geändert werden und in neuen Ausgaben dieses Dokuments enthalten sein, falls diese ggf. von der PGP Corporation zur Verfügung gestellt werden.

Nicht unterstützte Produkte von Dritten

Durch die Nutzung von Produkten, Softwareanwendungen, Treibern oder anderen Komponenten von Dritten („nicht unterstützte Produkte von Dritten“) für die Verwendung mit der PGP-Software und/oder durch die Nutzung von zugehörigen PGP-Befehlen oder zugehörigem PGP-Code, die Ihnen von der PGP Corporation nach eigenem Ermessen für die Verwendung mit nicht unterstützten Produkten von Dritten zur Verfügung gestellt wurden („PGP-Drittanbieterbefehle“), erkennen Sie an, dass die PGP-Software nicht für das nicht unterstützte Produkt von Dritten entwickelt und auch nicht offiziell mit diesem getestet wurde, sodass die PGP Corporation daher weder Support noch Garantien für PGP-Drittanbieterbefehle oder für die Kompatibilität der PGP-Software mit nicht unterstützten Produkten von Dritten bietet. DIE PGP-DRITTANBIETERBEFEHLE WERDEN OHNE MÄNGELGEWÄHR UND MIT ALLEN FEHLERN BEREITGESTELLT UND DAS GESAMTE RISIKO BEZÜGLICH ZUFRIEDENSTELLENDER QUALITÄT, LEISTUNG, GENAUIGKEIT UND AUFWAND LIEGT BEI IHNEN. DIE PGP CORPORATION LEHNT IM MAXIMAL ZULÄSSIGEN RAHMEN DES ANWENDBAREN RECHTS JEGLICHE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN ZUSICHERUNGEN, GARANTIEN UND BEDINGUNGEN AB, EINSCHLIESSLICH JEGLICHER GARANTIEN ODER BEDINGUNGEN DER MARKTGÄNGIGKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DER VERFÜGUNGSRECHTE, DER NICHTVERLETZUNG DER RECHTE DRITTER, DES UNGESTÖRTEN BESITZES UND DER GENAUIGKEIT VON PGP-DRITTANBIETERBEFEHLEN ODER DER KOMPATIBILITÄT DER PGP-SOFTWARE MIT NICHT UNTERSTÜTZTEN PRODUKTEN VON DRITTEN.

Inhalt

Informationen zu PGP Desktop 10.1 für Mac OS X 1

Neuheiten bei PGP Desktop für Mac OS X Version 10.1 2
Dieses Handbuch verwenden 3
„Zentral verwaltete“ und „Einzelplatz“-Benutzer 3
In diesem Handbuch verwendete Konventionen 4
Adressaten dieses Dokuments 5
Informationen zur Lizenzierung von PGP Desktop 5
Informationen zur Lizenzierung von PGP Desktop 5
Lizenzdetails prüfen 6
Ablauf der Lizenz 8
Hilfe und Support 8
Informationen zum Produkt 8
Kontaktinformationen 9

PGP Desktop-Grundlagen 11

PGP Desktop-Grundbegriffe 11
PGP-Produktkomponenten 11
In PGP Desktop verwendete Begriffe 13
Konventionelle Kryptografie und Kryptografie mit öffentlichen Schlüsseln 15
PGP Desktop erstmals verwenden 16

PGP Desktop installieren 19

Systemvoraussetzungen 19
PGP Desktop installieren und konfigurieren 19
Software installieren 19
PGP Desktop mit Boot Camp von Apple verwenden 20
Software-Upgrade 21
Lizenzierung von PGP Desktop 24
Einrichtungsassistenten ausführen 24
Integration mit Entourage 2008 24
Option zum Deinstallieren von PGP Desktop 25
PGP Desktop-Installation von einem Computer auf einen anderen übertragen 25

Benutzeroberfläche von PGP Desktop 27

Auf PGP Desktop-Funktionen zugreifen 27
Hauptbildschirm von PGP Desktop 28
PGP Desktop-Symbol in der Menüleiste verwenden 29
PGP-Dock-Symbol verwenden 30
Finder von Mac OS X verwenden 32

Notifier-Warnungen von PGP Desktop 32
PGP Desktop Notifier für Messaging 32
PGP Desktop und der Finder 39
Übersicht 39
Verschlüsseln, signieren oder verschlüsseln und signieren 40
Sicher löschen 42
Entschlüsseln/Verifizieren 42
PGP Virtual Disk-Laufwerke aktivieren oder deaktivieren 43
PGP-Schlüssel importieren 44
Öffentliche PGP-Schlüssel zum Schlüsselbund hinzufügen 45
Inhalt von PGP Zip-Archiven extrahieren 45
PGP-Protokoll anzeigen 46

Mit PGP Keys arbeiten 47

Schlüssel anzeigen 48
Smart-Schlüsselbunde erstellen 49
Schlüsselpaare erstellen 50
Schlüsseleinstellungen im Expertenmodus 52
Privaten Schlüssel schützen 54
Schlüssel und Schlüsselbunde schützen 54
Sicherungskopien von privaten Schlüsseln erstellen 55
Vorgehensweise bei verlorenen Schlüsseln 56
Öffentliche Schlüssel verteilen 56
Öffentliche Schlüssel auf einem Keyserver ablegen 57
Öffentliche Schlüssel in E-Mail-Nachrichten einfügen 58
Öffentliche Schlüssel in Dateien exportieren 59
Öffentliche Schlüssel anderer Personen erhalten 60
Öffentliche Schlüssel von einem Keyserver abrufen 60
Öffentliche Schlüssel aus E-Mail-Nachrichten übernehmen 61
Mit Keyservern arbeiten 62
Hauptschlüssel verwenden 63
Der Hauptschlüsselliste Schlüssel hinzufügen 64
Schlüssel aus der Hauptschlüsselliste löschen 64

PGP-Schlüssel verwalten 65

Schlüsseleigenschaften anzeigen und festlegen 66
Fotos hinzufügen und entfernen 66
Benutzernamen und E-Mail-Adressen in einem Schlüssel verwalten 68
Schlüssel und X.509-Zertifikate importieren 69
In S/MIME-E-Mail-Nachrichten enthaltene X.509-Zertifikate importieren 69
Passphrase ändern 70
Schlüssel, Benutzer-IDs und Signaturen löschen 71
Öffentliche Schlüssel deaktivieren und aktivieren 72
Einen öffentlichen Schlüssel verifizieren 72
Öffentliche Schlüssel signieren 74
Signaturen von öffentlichen Schlüsseln widerrufen 76
Vertrauen für Schlüsselvalidierungen gewähren 76
So stufen Sie einen Schlüssel als vertrauenswürdig ein 77

Mit Unterschlüsseln arbeiten 77
Separate Unterschlüssel verwenden 79
Unterschlüssel anzeigen 79
Neue Unterschlüssel erstellen 80
Schlüsselverwendung für Unterschlüssel festlegen 81
Unterschlüssel widerrufen 82
Unterschlüssel entfernen 82
Mit ADKs arbeiten 82
ADKs zu einem Schlüsselpaar hinzufügen 83
Einen ADK aktualisieren 83
ADKs entfernen 84
Mit Widerrufern arbeiten 84
Designierte Widerrufer zu Schlüsseln hinzufügen 84
Schlüssel widerrufen 85
Schlüssel teilen und wieder zusammenfügen 86
Geteilte Schlüssel erstellen 86
Geteilte Schlüssel wieder zusammenfügen 87
Vorgehensweise bei verloren gegangenen Schlüsseln oder Passphrasen 89
Schlüssel mit PGP Universal Server wiederherstellen 90
Schlüsselwiederherstellungsdaten erstellen 90
Schlüssel bei verloren gegangenen Schlüsseln bzw. Passphrasen wiederherstellen 93
Schlüssel schützen 94

E-Mail-Nachrichten sichern 97

E-Mail-Nachrichten mit PGP Desktop sichern 97
Eingehende Nachrichten 98
Informationen zu Anmerkungen für eingehende Nachrichten 100
Ausgehende Nachrichten 101
Gesendete Objekte auf IMAP-E-Mail-Servern sichern 101
Offline-Richtlinien verwenden 102
Dienste und Richtlinien 103
Dienste und Richtlinien anzeigen 104
Neue Messaging-Dienste erstellen 105
Eigenschaften des Messaging-Dienstes bearbeiten 108
Dienste deaktivieren oder aktivieren 108
Dienste löschen 109
Mehrere Dienste 109
Problembehebung bei PGP Messaging-Diensten 110
Neue Sicherheitsrichtlinien erstellen 112
Reguläre Ausdrücke in Richtlinien 118
Informationen und Beispiele zu Sicherheitsrichtlinien 120
Mit der Sicherheitsrichtlinienliste arbeiten 123
Sicherheitsrichtlinien bearbeiten 123
Adressenlisten-Richtlinien bearbeiten 124
Sicherheitsrichtlinien löschen 129
Reihenfolge der Richtlinien in der Liste ändern 130
PGP Desktop und SSL 130
Schlüsselmodi 132
Schlüsselmodus ermitteln 134

Schlüsselmodus ändern 134
PGP-Protokoll anzeigen 136
PGP-Skripte mit Entourage 2008 verwenden 137

Instant Messaging-Sitzungen sichern 139

Informationen zur Instant Messaging-Kompatibilität von PGP Desktop 139
Kompatibilität mit Instant Messaging-Clients 141
Informationen zu den für die Verschlüsselung verwendeten Schlüsseln 141
IM-Sitzungen verschlüsseln 141

E-Mail-Nachrichten mit PGP Viewer anzeigen 143

Übersicht über PGP Viewer 143
Unterstützte E-Mail-Clients 144
Verschlüsselte E-Mail-Nachrichten oder Dateien öffnen 145
E-Mail-Nachrichten in den Posteingang kopieren 146
E-Mail-Nachrichten exportieren 146
Einstellungen von PGP Viewer 147
Sicherheitsfunktionen in PGP Viewer 148

Laufwerke mit PGP Whole Disk Encryption schützen 149

Informationen zu PGP Whole Disk Encryption 150
Startlaufwerke verschlüsseln 152
Worin unterscheidet sich PGP Whole Disk Encryption von PGP Virtual Disk? 152
PGP Whole Disk Encryption lizenzieren 153
Ablauf der Lizenz 153
Laufwerk auf die Verschlüsselung vorbereiten 153
Unterstützte Laufwerkstypen 154
Unterstützte Tastaturen 155
Laufwerksintegrität vor der Verschlüsselung sicherstellen 156
Verschlüsselungsdauer berechnen 157
Pilotversuch zum Sicherstellen der Softwarekompatibilität durchführen 157
Authentifizierungsmethode für das Laufwerk bestimmen 158
Laufwerke verschlüsseln 158
Unterstützte Zeichen 159
Laufwerk verschlüsseln 159
Laufwerksfehler während der Verschlüsselung 162
Mit PGP Whole Disk Encryption verschlüsselte Laufwerke verwenden 163
Authentifizierung im PGP BootGuard-Bildschirm 164
Schutz von Laufwerken aufrechterhalten 165
Schlüsselinformationen auf verschlüsselten Laufwerken anzeigen 166
Systempartition ändern 166
Andere Benutzer zu verschlüsselten Laufwerken hinzufügen 166
Benutzer von verschlüsselten Laufwerken löschen 167
Benutzer-Passphrasen ändern 168
Verschlüsselte Laufwerke umschlüsseln 168
Sicherungskopien erstellen und Daten wiederherstellen 169

PGP Desktop von verschlüsselten Laufwerken deinstallieren 170
PGP Whole Disk Encryption in einer von einem PGP Universal Server verwalteten Umgebung verwenden 170
PGP Whole Disk Encryption verwalten 170
Wiederherstellungs-Token erstellen 171
Wiederherstellungs-Token verwenden 172
Daten von verschlüsselten Laufwerken wiederherstellen 172
Wiederherstellungsdatenträger erstellen und verwenden 173
Mit PGP Whole Disk Encryption verschlüsselte Laufwerke entschlüsseln 174
Wechseldatenträger auf anderen Systemen verwenden 175
Auf Daten auf verschlüsselten Wechseldatenträgern zugreifen 175
Spezielle Sicherheitsmaßnahmen von PGP Desktop 176
Löschung der Passphrase 176
Schutz des virtuellen Speichers 176
Schutz durch MSIM (Memory Static Ion Migration) 177
Weitere Sicherheitsaspekte 177
Technische Details zum Verschlüsseln von Startlaufwerken 178

PGP Virtual Disk-Laufwerke verwenden 181

Informationen zu PGP Virtual Disk-Laufwerken 182
Neue PGP Virtual Disk-Laufwerke erstellen 183
Eigenschaften von PGP Virtual Disk-Laufwerken anzeigen 186
Aktivierte PGP Virtual Disk-Laufwerke verwenden 187
PGP Virtual Disk-Laufwerke aktivieren 187
PGP Virtual Disk-Laufwerke deaktivieren 188
Aktivierungsspeicherort festlegen 188
PGP Virtual Disk-Laufwerke komprimieren 189
PGP Virtual Disk-Laufwerke umschlüsseln 189
Mit anderen Benutzern arbeiten 190
Konten anderer Benutzer zu einem PGP Virtual Disk-Laufwerk hinzufügen 191
Konten anderer Benutzer von einem PGP Virtual Disk-Laufwerk löschen 192
Konten anderer Benutzer deaktivieren und aktivieren 192
Lese-/Schreib- und Schreibschutzstatus ändern 193
Anderen Benutzern Administratorstatus gewähren 193
Benutzer-Passphrasen ändern 194
PGP Virtual Disk-Laufwerke löschen 195
PGP Virtual Disk-Laufwerke warten 195
PGP Virtual Disk-Laufwerke auf einem Remoteserver aktivieren 196
Sicherungskopien von PGP Virtual Disk-Laufwerken erstellen 196
PGP Virtual Disk-Laufwerke austauschen 197
PGP Virtual Disk-Verschlüsselungsalgorithmen 198
Spezielle Sicherheitsfunktionen von PGP Virtual Disk 199
Löschung der Passphrase 199
Schutz des virtuellen Speichers 199
Schutz durch MSIM (Memory Static Ion Migration) 199
Weitere Sicherheitsaspekte 200

Mit PGP Portable auf mobile Daten zugreifen 203

Auf Daten auf einem PGP Portable-Laufwerk zugreifen 203
Passphrase für ein PGP Portable-Laufwerk ändern 205
PGP Portable-Laufwerk deaktivieren 206

PGP Zip verwenden 207

Übersicht 207
PGP Zip-Archive erstellen 208
PGP Zip-Archive öffnen 210
Signierte PGP Zip-Archive verifizieren 210

Dateien mit PGP Shredder sicher löschen 213

Dateien und Ordner mit PGP Shredder sicher und endgültig löschen 213
Dateien über das PGP Shredder-Symbol sicher löschen 215
Dateien über das Symbol „Dateien sicher löschen“ in der Symbolleiste von PGP Desktop sicher löschen 215
Dateien über den Befehl „Sicher löschen“ im Menü „Datei“ sicher löschen 215
Dateien im Finder sicher löschen 216

PGP Desktop-Einstellungen festlegen 217

Auf PGP Desktop-Einstellungen zugreifen 217
Allgemeine Einstellungen 218
Schlüsseleinstellungen 220
Hauptschlüsseleinstellungen 222
Messaging-Einstellungen 223
Proxy-Optionen 226

Laufwerkseinstellungen 228
Benachrichtigungseinstellungen 229
Erweiterte Einstellungen 232

Mit Kennwörtern und Passphrasen arbeiten 233

Entscheidung über die Verwendung eines Kennwortes oder einer Passphrase 234
Die Passphrasen-Qualitätsanzeige 234
Starke Passphrasen erstellen 235
Vorgehensweise bei vergessenen Passphrasen 237
Passphrasen im Schlüsselanhänger speichern 238

PGP Desktop mit PGP Universal Server verwenden 239

Übersicht 240
Für PGP-Administratoren 241
Manuelle Bindung an einen PGP Universal Server 242

Index 243

1 Informationen zu PGP Desktop 10.1 für Mac OS X

PGP Desktop ist eine Sicherheitslösung, die Ihre Daten mittels Kryptografie vor unbefugtem Zugriff schützt.

PGP Desktop schützt Ihre Daten, wenn sie per E-Mail oder Instant Messaging (IM) gesendet werden. Sie können eine gesamte Festplatte oder Partition (unter Windows) verschlüsseln, damit alle Daten ständig geschützt sind, oder Sie können nur einen Teil der Festplatte mithilfe eines virtuellen Laufwerks verschlüsseln, auf dem Sie Ihre vertraulichsten Daten sicher speichern können. Sie können Ihre Dateien und Ordner sicher mit anderen Benutzern im Netzwerk gemeinsam nutzen. Eine beliebige Kombination von Dateien und Ordnern kann zur einfachen Verteilung oder Sicherung in einem verschlüsselten Paket komprimiert werden. Darüber hinaus können Sie mit PGP Desktop vertrauliche Dateien sicher löschen, damit niemand mehr auf sie zugreifen kann, sowie den freien Speicherplatz auf der Festplatte überschreiben, damit keine ungesicherten Dateifragmente zurückbleiben.

Erstellen Sie mit PGP Desktop PGP-Schlüsselpaare und verwalten Sie sowohl Ihre privaten Schlüsselpaare als auch die öffentlichen Schlüssel anderer Benutzer.

Damit Sie PGP Desktop optimal nutzen können, sollten Sie mit der *PGP Desktop-Terminologie* (siehe "*PGP Desktop-Grundbegriffe*" auf Seite 11) vertraut sein. Außerdem ist ein Grundwissen der konventionellen Kryptografie und der Kryptografie mit öffentlichen Schlüsseln erforderlich. Weitere Informationen hierzu finden Sie unter *Konventionelle Kryptografie und Kryptografie mit öffentlichen Schlüsseln* (auf Seite 15).

In diesem Kapitel

Neuheiten bei PGP Desktop für Mac OS X Version 10.1 2
Dieses Handbuch verwenden 3
Adressaten dieses Dokuments 5
Informationen zur Lizenzierung von PGP Desktop 5
Hilfe und Support 8

Neuheiten bei PGP Desktop für Mac OS X Version 10.1

PGP Desktop 10.1< enthält zahlreiche Verbesserungen und die folgenden neuen Funktionen, die auf der bewährten Technologie der PGP Corporation aufbauen.

Messaging

- Anmerkungen wurden verbessert. In einer von einem PGP Universal Server verwalteten Umgebung kann der Administrator jetzt die Position der Anmerkung, beispielsweise unter dem Nachrichtentext statt den Nachrichtentext umschließend, festlegen.
- Sie können jetzt Kopien gesendeter Nachrichten für IMAP-Konten schützen (diese Option steht nur bei eigenständigen Installationen zur Verfügung). Sie bietet zusätzliche Sicherheit, damit Sie vertrauliche E-Mail-Nachrichten schützen können, die Sie über das IMAP-Konto gesendet haben. Wählen Sie **Verschlüsseln**, **Verschlüsseln und Signieren** oder **Nur signieren** aus, wenn Sie E-Mail-Nachrichten schützen möchten, wenn sie in den IMAP-Ordner für gesendete Objekte kopiert werden.
- Der PGP Universal Server-Administrator kann in einer verwalteten Umgebung Richtlinien festlegen, um Ihnen die Möglichkeit zu geben, eine Verifizierung der Signaturen von eingehenden E-Mail-Nachrichten durchzuführen. Wenn die entsprechende Option aktiviert ist, wird im Microsoft Outlook- oder Lotus Notes-E-Mail-Client eine neue Schaltfläche und/oder eine neue Menüoption angezeigt. Die Schaltfläche oder Option weist den vom Administrator festgelegten Standardstatus auf. Sie können diese Einstellung falls nötig ändern.
- In einer verwalteten Umgebung hat der PGP Universal Server-Administrator möglicherweise bestimmte PGP Notifier-Einstellungen festgelegt (z. B. die Anzeige von Benachrichtigungen oder die Position des Notifier-Fensters).
- In einer S/MIME-E-Mail-Nachricht enthaltene X.509-Zertifikate, die an Sie gesendet wurden, können jetzt an den Schlüsselbund importiert werden. Auf diese Zertifikate werden dieselben Einstellungen angewendet, die Sie für gefundene öffentliche Schlüssel angegeben haben. Wenn dies entsprechend angegeben ist, extrahiert PGP Desktop das X.509-Zertifikat und importiert es dann an den Schlüsselbund. Wenn Sie E-Mail-Nachrichten mit importierten Zertifikaten verschlüsseln möchten, müssen Sie das Zertifikat manuell signieren.
- In einer verwalteten Umgebung hat der PGP Universal Server-Administrator u. U. eine Einstellung so festgelegt, dass in der Unzustellbarkeitsbestätigung weitere Informationen enthalten sind, wenn eine Nachricht blockiert wird. Kann PGP Desktop keinen Schlüssel für einen oder mehrere Empfänger in der Gruppenliste finden, werden die E-Mail-Adressen in den Fehlerinformationen der Unzustellbarkeitsbestätigung aufgeführt.

PGP Portable

- Ein Link für **Weitere Informationen** wird jetzt im Dialogfeld **PGP Portable** angezeigt, wenn Sie auf Daten auf dem Gerät zugreifen. Der Browser wird geöffnet und die Support-Website der PGP Corporation wird angezeigt.
- Sie können jetzt den verfügbaren Festplattenspeicher und die Gesamtgröße des PGP Portable Disk-Laufwerks nach der Aktivierung des Laufwerks anzeigen. Wenn Sie den Cursor ein paar Sekunden über das Dockelement platzieren, wird die PGP Notifier-Meldung eingeblendet und zeigt den Aktivierungsstatus des PGP Portable Disk-Laufwerks sowie die aktualisierten Informationen zum Festplattenspeicher an.

PGP Whole Disk Encryption

- Der AES-128- und AES-256-Algorithmus für PGP Desktop für Mac OS X wurden verbessert, um die Ver- und Entschlüsselungszeiten sowie die Laufwerkszugriffszeiten für verschlüsselte Laufwerke zu verbessern.
- Verbesserung zur Erzwingung der Verschlüsselung von Startlaufwerken gemäß Richtlinie. Dies beinhaltet die Erzwingung der Verschlüsselung, wenn sich die Richtlinie geändert hat (beispielsweise wenn Startlaufwerke zuvor nicht verschlüsselt werden mussten und der Administrator nun die Richtlinie dahingehend geändert hat, dass die Verschlüsselung erforderlich ist).

Dieses Handbuch verwenden

In diesem Handbuch finden Sie Informationen zur Konfiguration und zur Verwendung von Komponenten in PGP Desktop. Jedes Kapitel dieses Handbuchs widmet sich einer Komponente von PGP Desktop.

„Zentral verwaltete“ und „Einzelplatz“-Benutzer

Mit einem PGP Universal-Server können die Richtlinien und Einstellungen der Komponenten von PGP Desktop gesteuert werden. Diese Funktion wird häufig in Unternehmen genutzt, die PGP-Software verwenden. PGP Desktop-Benutzer werden in dieser Konfiguration als *zentral verwaltete* Benutzer bezeichnet, da die in ihrer PGP Desktop-Software zur Verfügung stehenden Einstellungen und Richtlinien von einem PGP-Administrator vorkonfiguriert wurden und über einen PGP Universal Server zentral verwaltet werden. Wenn Sie in einer zentral verwalteten Umgebung arbeiten, gibt es in Ihrem Unternehmen u. U. spezifische Nutzungsanforderungen. Beispielsweise kann zentral verwalteten Benutzern der Versand von E-Mail-Nachrichten im Klartext gestattet oder untersagt werden oder sie müssen ihre Laufwerke mit PGP Whole Disk Encryption verschlüsseln.

Benutzer, die nicht über einen PGP Universal-Server verwaltet werden, werden als *nicht verwaltete* oder *Einzelplatz*-Benutzer bezeichnet.

In diesem Handbuch wird die Verwendung von PGP Desktop in beiden Situationen beschrieben. Verwaltete Benutzer werden während der Arbeit mit dem Produkt jedoch möglicherweise feststellen, dass einige der hier beschriebenen Einstellungen in ihren Umgebungen nicht verfügbar sind. Weitere Informationen finden Sie unter *PGP Desktop mit PGP Universal Server verwenden* (auf Seite 239).

Vom PGP Universal Server-Administrator angepasste Funktionen

Wenn Sie PGP Desktop als „verwalteter" Benutzer in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, können einige Einstellungen vom Administrator festgelegt werden. Durch diese Einstellungen ändert sich u. U. die Anzeige bestimmter Funktionen in PGP Desktop.

- **Deaktivierte Funktionen**: Der PGP Universal Server-Administrator kann bestimmte Funktionen aktivieren oder deaktivieren. Beispielsweise kann der Administrator festlegen, dass PGP Zip-Archive oder durch PGP NetShare geschützte Ordner nicht erstellt werden können (unter Windows).

  Wenn eine Funktion deaktiviert wurde, wird das entsprechende Bedienelement auf der linken Seite nicht angezeigt und das Menü für diese Funktion steht nicht zur Verfügung. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Die Benutzeroberfläche von PGP Desktop sieht u. U. anders aus, wenn der Administrator die verfügbaren Funktionen angepasst hat.

In diesem Handbuch verwendete Konventionen

Die Bezeichnungen „Hinweis", „Achtung" und „Warnung" werden folgendermaßen verwendet:

Hinweise: Hinweise enthalten zusätzliche, wichtige Informationen. Ein Hinweis lenkt Ihre Aufmerksamkeit auf wichtige Aspekte des Produkts. Durch das Lesen der Hinweise können Sie Ihre Verwendung des Produkts optimieren.

Achtung: Mit „Achtung" gekennzeichnete Vorsichtsmaßnahmen zeigen die Möglichkeit von Datenverlust oder geringfügigen Sicherheitsverletzungen an. Ein solcher Warnhinweis informiert Sie über Situationen, in denen Probleme auftreten können, sofern keine Vorsichtsmaßnahmen getroffen werden. Beachten Sie Vorsichtsmaßnahmen unbedingt.

Warnung: Warnungen zeigen die Möglichkeit schwerwiegender Datenverluste oder umfangreicher Sicherheitsverletzungen an. Eine Warnung bedeutet, dass schwerwiegende Probleme auftreten können, sofern Sie nicht geeignete Maßnahmen ergreifen. Bitten nehmen Sie Warnungen sehr ernst.

Adressaten dieses Dokuments

Dieses Dokument ist für alle Personen bestimmt, die PGP Desktop für Mac OS X zum Schutz ihrer Daten verwenden werden.

Hinweis: Wenn Sie keine Erfahrung mit Kryptographie haben und einen Überblick über die Grundbegriffe und Konzepte von PGP Desktop wünschen, finden Sie weitere Informationen unter *Eine Einführung in die Kryptographie*. (Dieses Dokument wurde bei der Installation von PGP Desktop auf Ihrem System installiert.)

Informationen zur Lizenzierung von PGP Desktop

Die Funktionalität der PGP-Software wird mittels einer Lizenz aktiviert. Diese Lizenz legt gleichzeitig das Ablaufdatum der Software fest. Abhängig von der jeweiligen Lizenz sind einige oder alle Anwendungen der PGP Desktop-Produktfamilie aktiviert. Nachdem Sie die Lizenzinformationen eingegeben haben, müssen Sie die Software manuell oder online von der PGP Corporation autorisieren lassen.

Es gibt drei Arten von Lizenzen:

- **Bewertung**: Diese Art der Lizenz ist in der Regel zeitlich begrenzt und schließt u. U. nicht alle PGP Desktop-Funktionen ein.
- **Mietlizenz**: Diese Art der Lizenz ist in der Regel für einen Mietzeitraum von einem Jahr gültig. Während des Mietzeitraums erhalten Sie die aktuelle Version der PGP-Software sowie alle in diesem Zeitraum herausgegebenen Upgrades und Aktualisierungen.
- **Dauerlizenz**: Diese Art der Lizenz gestattet Ihnen eine zeitlich unbegrenzte Verwendung von PGP Desktop. Mit einer zusätzlich verfügbaren jährlichen Software-Versicherung, die jedes Jahr erneuert werden muss, erhalten Sie außerdem Upgrades und Aktualisierungen, die während des Versicherungszeitraums veröffentlicht werden.

Informationen zur Lizenzierung von PGP Desktop

So lizenzieren Sie PGP Desktop Führen Sie einen der folgenden Schritte aus:

- Wenn Sie in einer verwalteten Umgebung arbeiten, verwenden Sie wahrscheinlich bereits eine lizenzierte Kopie von PGP Desktop. Überprüfen Sie die Lizenzdetails gemäß der Beschreibung unter *Lizenzdetails prüfen* (auf Seite 6). Wenn Sie Fragen haben, wenden Sie sich an den PGP-Administrator.
- Wenn Sie nicht in einer verwalteten Umgebung arbeiten oder wenn Sie ein PGP-Administrator sind, überprüfen Sie die Lizenzdetails gemäß der Beschreibung unter *Lizenzdetails prüfen* (auf Seite 6). Falls Sie Ihre Kopie von PGP Desktop autorisieren müssen, gehen Sie wie unter *PGP Desktop für Mac OS X autorisieren* (auf Seite 7) beschrieben vor.

Lizenzdetails prüfen

So zeigen Sie die Details der PGP Desktop-Lizenz an

1. Öffnen Sie PGP Desktop.
2. Klicken Sie im Menü **PGP** auf **Lizenz**. Das Dialogfeld mit den Lizenzinformationen wird angezeigt. Das folgende Dialogfeld wird angezeigt:
   - **Name**: Der Name, unter dem die Lizenz registriert ist.
   - **Organisation**: Die Organisation, für die die Lizenz registriert ist.
   - **E-Mail**: Die E-Mail-Adresse, die der Lizenz zugeordnet ist.
   - **Typ**: Der Typ der Lizenz: Enterprise oder Home.
3. Klicken Sie auf **Details**. Die Details der Lizenz werden angezeigt.

Enterprise-Lizenz
Ablaufdatum: 07.08.10
Anzahl der Plätze: 500
Aktivierte Funktionen: PGP Virtual Disk, PGP Whole Disk Encryption, Mail-Plug-ins, PGP Messaging, Enterprise-Verwaltung
Deaktivierte Funktionen: Keine
OK

   - **Ablaufdatum**: Das Datum, an dem die Lizenz abläuft.
   - **Anzahl der Plätze**: Die Anzahl der Plätze, für die diese Lizenz gilt.
   - **Aktivierte Funktionen**: Die Komponenten, die bei der Lizenz aktiv sind.
   - **Deaktivierte Funktionen**: Die Komponenten, die bei der Lizenz *nicht* aktiv sind.

Hinweis: Wenn Sie die Kopie von PGP Desktop nicht autorisieren, steht nur eine begrenzte Anzahl von Funktionen zur Verfügung (PGP Zip und PGP Keys).

PGP Desktop für Mac OS X autorisieren

Wenn Sie eine neue Lizenznummer verwenden müssen oder die Lizenzautorisierung während der Konfiguration übersprungen haben, führen Sie die folgenden Schritte aus, um die Software zu aktivieren.

Vorbereitung

Nach dem Kauf von PGP Desktop haben Sie eine Auftragsbestätigung mit Lizenzierungsinformationen erhalten.

1. Öffnen Sie PGP Desktop.
2. Klicken Sie im Menü **PGP** auf **Lizenz**.
3. Klicken Sie auf **Lizenz ändern**.
4. Geben Sie den **Namen** und die **Organisation** genau so an, wie sie in der Auftragsbestätigung aufgeführt sind.
5. Geben Sie die E-Mail-Adresse **ein, die Sie für die Lizenzierung des Produkts verwenden möchten.**
6. Führen Sie einen der folgenden Schritte aus:
   - Geben Sie die 28-stellige Lizenznummer in die Felder **Lizenznummer** ein (z. B. DEMO1-DEMO2-DEMO3-DEMO4-DEMO5-ABC).

   Hinweis: Sie können Tippfehler vermeiden und die Autorisierung vereinfachen, indem Sie die gesamte Lizenznummer kopieren und den Mauszeiger in das erste Feld für die Lizenznummer setzen. Fügen Sie die Nummer dann ein. Die Lizenznummer wird automatisch richtig in alle sechs Felder für die **Lizenznummer eingefügt.**

   - Wenn Sie eine PGP Desktop-Lizenz erwerben möchten, wählen Sie **Jetzt erwerben** aus. In einem Webbrowser wird der PGP-Online-Store angezeigt.
7. Klicken Sie auf **Autorisieren**.
8. Klicken Sie nach der Autorisierung der Lizenz auf **OK**, um den Vorgang abzuschließen.

Lizenzautorisierungsfehler beheben

Fehler, die während der Autorisierung der Software ausgegeben werden, müssen entsprechend ihrer Ursache behoben werden. Lösungsvorschläge finden Sie im *PGP-Supportportal* (*https://support.pgp.com*) im Abschnitt mit Informationen zur Lizenzierung von PGP Desktop 10.1, *HOWTO: License PGP Desktop 10.1*.

Ablauf der Lizenz

Wenn Ihre PGP Desktop-Lizenz abgelaufen ist, wird beim Starten von PGP Desktop eine Nachricht zum Ablaufdatum der PGP-Lizenz angezeigt. Weitere Informationen zu den Auswirkungen einer abgelaufenen Lizenz auf die Funktionalität von PGP Desktop finden Sie in den folgenden Abschnitten.

PGP Desktop Email

- Ausgehende E-Mail-Nachrichten werden nicht mehr verschlüsselt gesendet.

PGP Virtual Disk

- Der Zugriff auf PGP Virtual Disk-Laufwerke ist nur im schreibgeschützten Modus möglich. Im schreibgeschützten Modus können Daten von einem PGP Virtual Disk-Laufwerk kopiert werden, jedoch ist das Kopieren von Daten auf ein PGP Virtual Disk-Laufwerk nicht möglich.

PGP Whole Disk Encryption

Alle Festplatten, die mit PGP Desktop verschlüsselt wurden, werden automatisch 90 Tage nach Ablauf der Lizenz entschlüsselt.

Hilfe und Support

Informationen zu weiteren Ressourcen finden Sie in diesen Abschnitten.

Informationen zum Produkt

Sofern nicht anders angegeben, wird eine Online-Hilfe installiert, die in PGP Desktop zur Verfügung steht. Darüber hinaus sind Versionshinweise verfügbar, die kurzfristig bereitgestellte Informationen enthalten können, die nicht in der Produktdokumentation zu finden sind. Das Benutzerhandbuch und Handbücher für den Schnelleinstieg, die als Adobe Acrobat PDF-Dateien zur Verfügung gestellt werden, sind im PGP-Supportportal im Bereich für *Dokumentation* (*https://pgp.custhelp.com/app/docs*) zu finden.

Nach der Veröffentlichung von PGP Desktop werden zusätzliche Informationen zum Produkt der Online-Wissensdatenbank hinzugefügt, die über die Website des *PGP-Supportportals* (*https://support.pgp.com*) verfügbar ist.

Kontaktinformationen

Kontaktaufnahme mit dem technischen Support

- Informationen zu PGP-Supportoptionen und zur Kontaktaufnahme mit dem technischen PGP-Support finden Sie auf der *Support-Homepage der PGP Corporation* (*https://support.pgp.com*).
- Greifen Sie auf die PGP Support Knowledge Base zu oder fordern Sie technischen PGP-Support an, indem Sie die Website des *PGP-Supportportals* (*https://support.pgp.com*) aufrufen. **Der Zugriff auf Teile der PGP Support Knowledge Base ist ohne Supportvertrag möglich. Wenn Sie technischen Support anfordern möchten, ist dieser jedoch erforderlich.**
- Greifen Sie auf die PGP-Supportforen über den *PGP-Support* (*http://forum.pgp.com*) zu. Hierbei handelt es sich um Supportforen der Benutzer-Community, die von der PGP Corporation gehostet werden.

Kontaktaufnahme mit dem Kundendienst

- Unterstützung für Bestellungen, Downloads und zur Lizenzierung erhalten Sie vom *Kundendienst der PGP Corporation* (*https://pgp.custhelp.com/app/cshome*).

Kontaktaufnahme mit anderen Abteilungen

- Informationen zu weiteren Möglichkeiten der Kontaktaufnahme mit der PGP Corporation finden Sie auf der *Kontaktseite der PGP Corporation* (*http://www.pgp.com/about_pgp_corporation/contact/index.html*).
- Allgemeine Informationen zur PGP Corporation finden Sie auf der *PGP-Website* (*http://www.pgp.com*).

2 PGP Desktop-Grundlagen

In diesem Abschnitt werden die Grundbegriffe von PGP Desktop beschrieben und einige wichtige Grundlagen zur Kryptographie erläutert.

In diesem Kapitel

PGP Desktop-Grundbegriffe 11
Konventionelle Kryptografie und Kryptografie mit öffentlichen Schlüsseln15
PGP Desktop erstmals verwenden 16

PGP Desktop-Grundbegriffe

Zur optimalen Nutzung von PGP Desktop sollten Sie sich mit den Begriffen im folgenden Abschnitt vertraut machen.

PGP-Produktkomponenten

PGP Desktop und die Komponenten der Anwendung werden in der folgenden Liste beschrieben. Abhängig von der Lizenz stehen möglicherweise nicht alle Funktionen zur Verfügung. Weitere Informationen finden Sie unter *Informationen zur Lizenzierung von PGP Desktop* (auf Seite 5).

- **PGP Desktop**: Eine Softwareanwendung, die Daten kryptografisch vor unbefugtem Zugriff schützt. PGP Desktop ist für Mac OS X und Windows verfügbar.
    - **PGP Messaging**: Eine Funktion von PGP Desktop, die alle von Ihnen verwendeten E-Mail-Clients automatisch und transparent über von Ihnen erstellte Richtlinien unterstützt. PGP Desktop verwendet hierzu eine neue Proxy-Technologie. Die ältere Plug-in-Technologie steht ebenfalls zur Verfügung. Außerdem schützt PGP Messaging viele IM-Clients, z. B. AIM und iChat (bei beiden Benutzern muss PGP Messaging aktiviert sein).

- **PGP Whole Disk Encryption**: PGP Whole Disk Encryption ist eine Komponente von PGP Desktop, mit der gesamte Festplatten oder Partitionen (unter Windows) einschließlich des Startdatensatzes verschlüsselt werden können. Dadurch werden alle Dateien geschützt, wenn Sie sie nicht verwenden. PGP Whole Disk Encryption und PGP Virtual Disk-Laufwerke können zusammen auf einem System eingesetzt werden. Unter Windows können vollständig verschlüsselte Laufwerke mit einer Passphrase oder mit einem Schlüsselpaar auf einem USB-Token geschützt werden, um die Sicherheit zu erhöhen.
- **PGP NetShare**: Eine Funktion von PGP Desktop für Windows, mit der Sie Dateien und Ordner sicher und transparent für bestimmte Personen freigeben können. PGP NetShare-Benutzer können ihre Dateien und Ordner einfach schützen, indem sie diese in einem Ordner ablegen, der als geschützt gekennzeichnet wird.
- **PGP Keys**: Eine Funktion von PGP Desktop, die Ihnen die vollständige Kontrolle über Ihre eigenen PGP-Schlüssel und die Schlüssel von Personen gibt, mit denen Sie E-Mail-Nachrichten sicher austauschen.
- **PGP Virtual Disk-Laufwerke**: PGP Virtual Disk-Laufwerke stellen eine Funktion von PGP Desktop dar, mit der Sie einen Teil der Festplatte als verschlüsseltes virtuelles Laufwerk verwenden können. PGP Virtual Disk-Laufwerke können mit einem Schlüssel oder mit einer Passphrase geschützt werden. Sie können sogar weitere Benutzer für ein Laufwerk erstellen und dadurch autorisierten Personen den Zugriff auf das Laufwerk gestatten. Die PGP Virtual Disk-Funktion bietet sich besonders für Laptops an. Sollte der Laptop verloren gehen oder gestohlen werden, sind vertrauliche Daten, die auf dem PGP Virtual Disk-Laufwerk gespeichert sind, vor unbefugtem Zugriff geschützt.
- **PGP Shred**: Eine Funktion von PGP Desktop, mit der Sie Daten sicher vom System löschen können. Die Dateien werden von PGP Shred überschrieben und können selbst mit Software für die Datenwiederherstellung nicht wiederhergestellt werden.
- **PGP Viewer**: Mit PGP Viewer können Sie Nachrichten *außerhalb* des E-Mail-Stroms entschlüsseln, verifizieren und anzeigen.
- **PGP Zip**: Eine Funktion von PGP Desktop, mit der Sie eine beliebige Kombination von Dateien und Ordnern für die Datenübertragung oder -sicherung zu einem einzigen verschlüsselten, komprimierten Paket zusammenfassen können. Sie können ein PGP Zip-Archiv an einen PGP-Schlüssel oder an eine Passphrase verschlüsseln.

- **PGP Universal**: Ein Tool für Unternehmen, mit dem E-Mail-Nachrichten der Mitarbeiter automatisch und transparent gesichert werden. Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, werden die Messaging-Richtlinien und andere Einstellungen möglicherweise vom PGP-Administrator der Organisation gesteuert.

- **PGP Global Directory**: Ein kostenloser öffentlicher Keyserver, der von der PGP Corporation gehostet wird. Das PGP Global Directory ermöglicht den schnellen und einfachen Zugriff auf PGP-Schlüssel. Es nutzt eine Keyserver-Technologie der nächsten Generation, um die E-Mail-Adresse eines Schlüssels abzufragen (und dadurch zu prüfen, ob der Besitzer der E-Mail-Adresse den Schlüssel tatsächlich übermitteln möchte) und den Benutzern die Verwaltung ihrer Schlüssel zu ermöglichen. Durch die Verwendung des PGP Global Directory haben Sie bessere Chancen, den gültigen öffentlichen Schlüssel einer Person zu finden, der Sie sichere Nachrichten senden möchten. PGP Desktop wurde für die enge Zusammenarbeit mit dem PGP Global Directory entwickelt.

In PGP Desktop verwendete Begriffe

Bevor Sie PGP Desktop verwenden, sollten Sie sich mit den folgenden Begriffen vertraut machen.

- **Entschlüsseln:** Der Vorgang, bei dem verschlüsselte (chiffrierte) Daten wieder in lesbare Daten umgewandelt werden. Wenn Sie Daten empfangen, die von einer anderen Person mit Ihrem öffentlichen Schlüssel verschlüsselt wurden, können Sie sie mit Ihrem privaten Schlüssel entschlüsseln.
- **Verschlüsseln:** Der Vorgang, bei dem Daten chiffriert werden, damit sie für unbefugte Personen, die Zugriff auf die Daten erhalten, nicht verwendet werden können. Die Daten werden so chiffriert, dass sie bedeutungslos sind.
- **Signieren:** Der Vorgang, bei dem eine digitale Signatur mit Ihrem privaten Schlüssel auf Daten angewendet wird. Da Daten, die mit Ihrem privaten Schlüssel signiert wurden, nur durch Ihren öffentlichen Schlüssel verifiziert werden können, wird durch die Verifizierung der signierten Daten mit Ihrem öffentlichen Schlüssel belegt, dass Ihr privater Schlüssel die Daten signiert hat und die Daten daher von Ihnen stammen.
- **Verifizieren:** Der Vorgang, mit dem bewiesen wird, dass der private Schlüssel einer Person zum digitalen Signieren der Daten verwendet wurde. Dies geschieht mithilfe des öffentlichen Schlüssels der betreffenden Person. Da Daten, die mit einem privaten Schlüssel signiert wurden, nur durch den entsprechenden öffentlichen Schlüssel verifiziert werden können, beweist die Tatsache, dass ein bestimmter öffentlicher Schlüssel signierte Daten verifizieren kann, dass der Signierer wirklich der Besitzer des privaten Schlüssels ist.

- **Schlüsselpaar:** Eine Kombination aus privatem und öffentlichem Schlüssel. Wenn Sie einen PGP-Schlüssel erstellen, wird eigentlich ein Schlüsselpaar erstellt. Da Ihr Schlüsselpaar neben dem privaten und dem öffentlichen Schlüssel auch Ihren Namen und Ihre E-Mail-Adresse enthält, können Sie es sich eher als digitalen Ausweis vorstellen. Es identifiziert Sie in der digitalen Welt, so wie Sie durch Ihren Personalausweis oder Ihren Reisepass in der realen Welt ausgewiesen werden.
- **Privater Schlüssel:** Der Schlüssel, den Sie äußerst geheim halten müssen. Sie können nur mit Ihrem privaten Schlüssel Daten entschlüsseln, die mit Ihrem öffentlichen Schlüssel verschlüsselt wurden. Darüber hinaus kann nur mit Ihrem privaten Schlüssel eine digitale Signatur erstellt werden, die mit Ihrem öffentlichen Schlüssel verifiziert werden kann.

  Achtung: Geben Sie Ihren privaten Schlüssel oder dessen Passphrase niemals an andere weiter. Bewahren Sie Ihren privaten Schlüssel sicher auf.

- **Öffentlicher Schlüssel:** Der Schlüssel, den Sie an andere Personen ausgeben, damit diese Ihnen geschützte Nachrichten (Nachrichten, die nur mit Ihrem privaten Schlüssel entschlüsselt werden können) senden und Ihre digitale Signatur verifizieren können. Öffentliche Schlüssel sollten möglichst weit verbreitet werden.

  Der öffentliche und der private Schlüssel sind mathematisch betrachtet miteinander verwandt. Es ist jedoch unmöglich, aus dem öffentlichen Schlüssel einer Person deren privaten Schlüssel zu ermitteln.
- **Keyserver:** Ein Aufbewahrungsort für Schlüssel. Einige Unternehmen betreiben eigene Keyserver für die öffentlichen Schlüssel ihrer Mitarbeiter, damit diese ihre öffentlichen Schlüssel abrufen und geschützt miteinander kommunizieren können. Das *PGP Global Directory* (*https://keyserver.pgp.com*) ist ein kostenloser, frei zugänglicher Keyserver, der von der PGP Corporation gehostet wird.
- **Smartcards und Token:** Smartcards und Token sind tragbare Geräte, auf denen Sie ein PGP-Schlüsselpaar erstellen oder ein PGP-Schlüsselpaar kopieren können. Wenn Sie ein PGP-Schlüsselpaar auf einer Smartcard oder einem Token erstellen, wird die Sicherheit erhöht, da der Besitz der Smartcard oder des Tokens eine Voraussetzung für das Verschlüsseln, Signieren, Entschlüsseln oder Verifizieren ist. Selbst wenn eine unbefugte Person Zugriff auf Ihren Computer erlangt, bleiben Ihre verschlüsselten Daten weiterhin geschützt, da Sie Ihr PGP-Schlüsselpaar auf der Smartcard oder dem Token stets mit sich führen. Kopieren Sie das PGP-Schlüsselpaar auf eine Smartcard oder ein Token, wenn Sie es auf einem anderen System als dem Hauptsystem verwenden möchten oder wenn Sie es sichern bzw. Ihren öffentlichen Schlüssel weitergeben möchten. Smartcards und Token stehen bei der Verwendung von PGP Desktop für Mac OS X nicht als Schlüsselspeicher zur Verfügung.

Konventionelle Kryptografie und Kryptografie mit öffentlichen Schlüsseln

Konventionelle Kryptografie verwendet zum Verschlüsseln und Entschlüsseln von Daten dieselbe Passphrase. Die konventionelle Kryptografie eignet sich hervorragend für stationäre Daten, da die Verschlüsselung und Entschlüsselung sehr schnell erfolgt. Sie ist jedoch nicht besonders für Situationen geeignet, in denen Sie verschlüsselte Daten an andere Personen senden müssen, insbesondere wenn Sie mit diesen Personen noch nie Kontakt hatten.

Kryptografie mit öffentlichen Schlüsseln verwendet für das Verschlüsseln und Entschlüsseln zwei Schlüssel (ein so genanntes Schlüsselpaar). Einer der beiden Schlüssel ist Ihr privater Schlüssel, der, wie bereits der Name besagt, geheim gehalten und äußerst vertraulich behandelt werden muss. Der andere Schlüssel ist Ihr öffentlicher Schlüssel. Dieser Schlüssel kann, wie bereits der Name besagt, ohne Bedenken weitergegeben werden. Er ist sogar zur öffentlichen Weitergabe bestimmt.

Die Kryptografie mit öffentlichem Schlüssel funktioniert folgendermaßen: Angenommen, Sie und Ihre Cousine in einer anderen Stadt möchten persönliche Nachrichten austauschen. Sie beide verwenden PGP Desktop. Zunächst müssen Sie beide ein Schlüsselpaar erstellen: einen privaten Schlüssel und einen öffentlichen Schlüssel. Sie halten den privaten Schlüssel geheim und senden den öffentlichen Schlüssel an einen öffentlichen Keyserver wie das PGP Global Directory (keyserver.pgp.com), einer allgemein zugänglichen Einrichtung zum Verteilen öffentlicher Schlüssel. (Einige Unternehmen verfügen über eigene, nicht allgemein zugängliche Keyserver.)

Sobald sich die öffentlichen Schlüssel auf dem Keyserver befinden, können Sie den öffentlichen Schlüssel Ihrer Cousine von dort abrufen. Auf die gleiche Weise verfährt Ihre Cousine mit Ihrem öffentlichen Schlüssel (zum Austauschen öffentlicher Schlüssel gibt es auch andere Möglichkeiten; weitere Informationen hierzu finden Sie unter *Mit PGP-Schlüsseln arbeiten* (siehe "*Mit PGP Keys arbeiten*" auf Seite 47)). Dies ist wichtig, da Sie zum Senden einer verschlüsselten E-Mail-Nachricht, die nur Ihre Cousine entschlüsseln kann, die Nachricht mit dem **öffentlichen Schlüssel Ihrer Cousine verschlüsseln. Dieses Verfahren funktioniert, da eine Nachricht, die mit dem öffentlichen Schlüssel Ihrer Cousine verschlüsselt wurde, nur mit dem privaten Schlüssel Ihrer Cousine wieder entschlüsselt werden kann. Obwohl Sie im Besitz des öffentlichen Schlüssels Ihrer Cousine sind, können Sie die Nachricht nicht mehr entschlüsseln, nachdem sie mit ihrem öffentlichem Schlüssel verschlüsselt wurde. Nur mit dem privaten Schlüssel können Daten entschlüsselt werden, die zuvor mit dem entsprechenden öffentlichen Schlüssel verschlüsselt wurden.**

Der öffentliche und der private Schlüssel sind mathematisch betrachtet miteinander verwandt. Es ist jedoch nicht möglich, den privaten Schlüssel einer Person anhand des öffentlichen Schlüssels zu ermitteln.

PGP Desktop erstmals verwenden

Die PGP Corporation empfiehlt die folgende Vorgehensweise für die ersten Schritte mit PGP Desktop:

1 Installieren Sie PGP Desktop auf dem Computer.

Falls Sie ein Benutzer in einem Unternehmen sind, hat der PGP-Administrator möglicherweise spezifische Installationsanleitungen für Sie vorbereitet oder das PGP-Installationsprogramm mit bestimmten Einstellungen konfiguriert. In jedem Fall stellt die Installation den ersten Schritt dar.

2 Führen Sie die Einrichtung mit dem Einrichtungsassistenten durch.

Nachdem Sie PGP Desktop installiert und den Computer neu gestartet haben, wird der Einrichtungsassistent geöffnet. Sie erhalten Unterstützung bei folgenden Aufgaben:

- Lizenzierung von PGP Desktop
- Erstellen eines Schlüsselpaars mit oder ohne Unterschlüsseln (falls noch kein Schlüsselpaar vorhanden ist).
- Veröffentlichen Ihres öffentlichen Schlüssels im PGP Global Directory
- Aktivieren von PGP Messaging
- Anzeigen eines Überblicks über weitere Funktionen

Wenn ein PGP-Administrator das Installationsprogramm von PGP Desktop konfiguriert hat, können mit dem Einrichtungsassistenten möglicherweise noch andere Aufgaben durchgeführt werden.

3 Tauschen Sie öffentliche Schlüssel mit anderen Personen aus.

Nachdem Sie ein Schlüsselpaar erstellt haben, können Sie sichere Nachrichten an andere PGP Desktop-Benutzer senden und von diesen empfangen (nachdem Sie Ihre öffentlichen Schlüssel untereinander ausgetauscht haben). Sie können auch die PGP Desktop-Funktionen für den Laufwerkschutz verwenden.

Das Austauschen öffentlicher Schlüssel ist ein wichtiger erster Schritt. Damit Sie sichere Nachrichten an andere Personen senden können, benötigen Sie eine Kopie des öffentlichen Schlüssels des Empfängers. Wenn der Empfänger mit einer sicheren Nachricht antworten möchte, benötigt er eine Kopie Ihres öffentlichen Schlüssels. Falls Sie Ihren öffentlichen Schlüssel noch nicht mit dem Einrichtungsassistenten in das PGP Global Directory übertragen haben, holen Sie dies jetzt nach. Wenn Sie nicht über den öffentlichen Schlüssel einer Person verfügen, an die Sie Nachrichten senden möchten, sollten Sie zunächst das PGP Global Directory durchsuchen. PGP Desktop übernimmt diese Aufgabe für Sie. Wenn Sie eine E-Mail-Nachricht senden, sucht die Anwendung automatisch nach den Schlüsseln anderer PGP Desktop-Benutzer und verifiziert diese. Danach wird Ihre Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und gesendet.

4 Überprüfen Sie die öffentlichen Schlüssel, die Sie von nicht vertrauenswürdigen Keyservern erhalten.

Wenn Sie einen öffentlichen Schlüssel von einem nicht vertrauenswürdigen Keyserver beziehen, vergewissern Sie sich, dass er nicht verfälscht wurde und tatsächlich dem angeblichen Besitzer gehört. Vergleichen Sie zu diesem Zweck mit PGP Desktop den eindeutigen Fingerabdruck auf Ihrer Kopie des öffentlichen Schlüssels der Person mit dem Fingerabdruck auf dem Schlüssel dieser Person (z. B. indem Sie den Besitzer des Schlüssels anrufen und sich die Daten des Fingerabdrucks vorlesen lassen, sodass Sie sie vergleichen können). Schlüssel von vertrauenswürdigen Keyservern wie dem PGP Global Directory sind bereits verifiziert.

5 Sichern Sie Ihre E-Mail-Nachrichten, Dateien und Instant Message-Sitzungen.

Nachdem Sie Ihr Schlüsselpaar erstellt und die öffentlichen Schlüssel ausgetauscht haben, können Sie beginnen, E-Mail-Nachrichten und Dateien zu verschlüsseln, zu entschlüsseln, zu signieren und zu verifizieren. Mit der Funktion für sichere IM-Sitzungen werden automatisch eigene Schlüssel erstellt. Die Funktion kann daher verwendet werden, bevor Sie Ihr Schlüsselpaar erstellen. Die einzige Voraussetzung für sichere Sitzungen ist, dass sie mit anderen PGP Desktop-Benutzern stattfinden.

6 Achten Sie auf Informationsfenster von PGP Desktop Notifier.

Wenn Sie E-Mail-Nachrichten senden oder empfangen oder andere PGP Desktop-Funktionen ausführen, zeigt PGP Desktop Notifier in einer von Ihnen festgelegten Ecke des Bildschirms Informationsfenster an. In diesen Fenstern von PGP Notifier werden Aktionen gemeldet, die von PGP Desktop durchgeführt wurden bzw. durchgeführt werden. Wenn Sie sich mit dem Senden und Empfangen von Nachrichten vertraut gemacht haben, können Sie die Optionen für PGP Notifier ändern oder die Funktion deaktivieren.

7 Nachdem Sie einige Nachrichten gesendet oder empfangen haben, prüfen Sie die Protokolle, um sicherzustellen, dass alles ordnungsgemäß funktioniert.

Wenn Sie mehr Informationen benötigen, als von PGP Notifier angezeigt werden, finden Sie im PGP-Protokoll detaillierte Angaben zu allen Messaging-Vorgängen.

8 Ändern Sie bei Bedarf die Messaging-Richtlinien.

E-Mail-Nachrichten werden automatisch und nahtlos gesendet und empfangen, wenn die Messaging-Richtlinien von PGP Desktop ordnungsgemäß konfiguriert wurden. Wenn sich der Schlüssel des Empfängers im PGP Global Directory befindet, verwenden die Standardrichtlinien von PGP Desktop eine *opportunistische* Verschlüsselung. Das bedeutet, dass PGP Desktop die Nachricht automatisch verschlüsselt, wenn die Anwendung über alle erforderlichen Informationen verfügt (z. B. den **verifizierten** öffentlichen Schlüssel des Empfängers). Andernfalls wird die Nachricht im *Klartext* (unverschlüsselt) *gesendet. Die Standardrichtlinien von PGP Desktop ermöglichen optional auch eine erzwungene* Verschlüsselung. Dadurch **muss** eine Nachricht verschlüsselt werden, wenn in der Betreffzeile der Text „[PGP]“ angegeben wird. Wenn keine verifizierten Schlüssel gefunden werden, wird die Nachricht nicht gesendet und es wird ein Notifier-Fenster mit einer entsprechenden Meldung angezeigt.

9 Verwenden Sie die anderen Funktionen von PGP Desktop.

Sie können nicht nur die Messaging-Funktionen von PGP Desktop nutzen, sondern die Anwendung auch zum Sichern von Laufwerken verwenden:

- Verschlüsseln Sie mit **PGP Whole Disk Encryption** ein Startlaufwerk, eine Datenträgerpartition (Windows), externe Laufwerke oder USB-Flash-Laufwerke. Alle Dateien auf der Festplatte oder Partition werden gesichert und während der Verwendung entsprechend ver- und entschlüsselt. Dieser Prozess läuft für Sie völlig transparent ab.
- Erstellen Sie mit **PGP Virtual Disk** ein sicheres „virtuelles Laufwerk“. Dieses virtuelle Laufwerk kann wie ein Tresor für Ihre Dateien verwendet werden. Deaktivieren und sperren Sie das virtuelle Laufwerk mit PGP Desktop, dem Windows Explorer oder dem Finder von Mac OS X, sodass Ihre Dateien sicher sind, selbst wenn der Rest des Computers nicht gesperrt ist.
- Erstellen Sie mit **PGP Zip** komprimierte und verschlüsselte PGP Zip-Archive. Auf diese Weise können Sie Dateien effizient und sicher weitergeben oder speichern.
- Löschen Sie mit **PGP Shredder** vertrauliche Dateien, die Sie nicht mehr benötigen. PGP Shredder entfernt die Dateien vollständig von der Festplatte und sie können danach nicht mehr wiederhergestellt werden.

3 PGP Desktop installieren

In diesem Abschnitt wird beschrieben, wie Sie PGP Desktop auf dem Computer installieren und die ersten Schritte mit der Anwendung ausführen.

In diesem Kapitel

Systemvoraussetzungen 19
PGP Desktop installieren und konfigurieren 19
Option zum Deinstallieren von PGP Desktop 25
PGP Desktop-Installation von einem Computer auf einen anderen übertragen 25

Systemvoraussetzungen

Für die Installation von PGP Desktop unter Mac OS X gelten folgende Mindestanforderungen an das System:

- Apple Mac OS X10.5.x oder 10.6.x (Intel)
- 512 MB RAM
- 64 MB Festplattenspeicher

PGP Desktop installieren und konfigurieren

In diesem Abschnitt finden Sie Informationen zum Installieren oder Aktualisieren von PGP Desktop sowie zum Einrichtungsassistenten.

Software installieren

Hinweis: Sie müssen auf dem System über Administratorrechte verfügen, um die Aktualisierung installieren zu können.

Das Installationsprogramm von PGP Desktop unterstützt Sie bei der Installation.

So installieren Sie PGP Desktop unter Mac OS X

1. Beenden Sie alle anderen Anwendungen.
2. Aktivieren Sie das PGP DiskCopy-Image.
3. Doppelklicken Sie auf `PGP.pkg`.
4. Folgen Sie den Anleitungen auf dem Bildschirm.
5. Starten Sie das System neu, wenn Sie dazu aufgefordert werden.

Hinweis: Falls Sie in einer Domäne arbeiten, die durch einen PGP Universal Server geschützt ist, hat der PGP-Administrator das Installationsprogramm für PGP Desktop möglicherweise mit bestimmten Funktionen und/oder Einstellungen vorkonfiguriert. Wenn der PGP-Administrator das System für die stille Anmeldung eingerichtet hat, wird das Windows-Domänenkennwort für alle Passphrasen-Anforderungen in PGP Desktop verwendet. Wenn dies per Richtlinie festgelegt ist, kann PGP Whole Disk Encryption automatisch die Verschlüsselung des Laufwerks starten, wenn Sie das Windows-Kennwort eingeben.

PGP Desktop mit Boot Camp von Apple verwenden

Boot Camp von Apple ist mit PGP Desktop 10.0 oder höher kompatibel. Wenn Sie PGP Desktop mit Boot Camp verwenden möchten, müssen Sie die Software installieren und das Laufwerk in einer bestimmten Reihenfolge verschlüsseln.

Vergewissern Sie sich bevor Sie beginnen, dass Boot Camp ordnungsgemäß installiert ist. Informationen zum Einrichten von Boot Camp finden Sie im Dokument *Boot Camp-Installation und Konfiguration* (*http://manuals.info.apple.com/en/boot_camp_install-setup.pdf*) von Apple. Damit Sie Windows XP in der Windows-Partition verwenden können, muss die Partition im FAT32-Format konfiguriert sein. PGP Desktop unterstützt nicht die Installation von Linux auf einer Partition in Boot Camp.

Wenn Sie das Laufwerk entschlüsseln müssen, empfiehlt die PGP Corporation, diesen Vorgang auf der Mac OS X-Partition auszuführen.

Weitere Informationen zum Verwenden von PGP Desktop mit Apple Boot Camp finden Sie im *PGP-Wissensdatenbankartikel 1697* (*https://support.pgp.com/?faq=1697*).

Hinweis: Stellen Sie sicher, dass das Laufwerk nicht verschlüsselt ist (andernfalls müssen Sie das Laufwerk vor der Installation von Boot Camp entschlüsseln). Deinstallieren Sie dann PGP Desktop.

So verwenden Sie Boot Camp von Apple in einer eigenständigen Umgebung

1. Installieren Sie Boot Camp von Apple.

2 Installieren Sie PGP Desktop auf der Mac OS X-Partition und schließen Sie die Installation mit dem Einrichtungsassistenten ab.

3 Führen Sie den Systemstart auf der Windows-Partition durch und installieren Sie PGP Desktop unter Windows. Führen Sie nicht den Einrichtungsassistenten auf der Windows-Partition aus.

4 Führen Sie den Systemstart auf der Mac OS X-Partition durch und verschlüsseln Sie das Laufwerk. Wenn Sie den Verschlüsselungsvorgang unter Mac OS X anhalten, haben Sie an dieser Stelle die Möglichkeit, den Systemstart auf der Windows-Partition durchzuführen, jedoch muss die Verschlüsselung unter Mac OS X fortgesetzt werden.

So verwenden Sie Boot Camp von Apple in einer von einem PGP Universal Server verwalteten Umgebung

1 Installieren Sie Boot Camp von Apple.

2 Führen Sie den Systemstart auf der Windows-Partition durch und installieren Sie PGP Desktop unter Windows. Führen Sie nicht den Einrichtungsassistenten auf der Windows-Partition aus.

3 Installieren Sie PGP Desktop auf der Mac OS X-Partition und führen Sie die Anmeldung mit dem Einrichtungsassistenten durch.

4 Beginnen Sie während der Ausführung der Mac OS X-Partition mit der Verschlüsselung des Laufwerks. Wenn Sie den Verschlüsselungsvorgang unter Mac OS X anhalten, haben Sie an dieser Stelle die Möglichkeit, den Systemstart auf der Windows-Partition durchzuführen, jedoch muss die Verschlüsselung unter Mac OS X fortgesetzt werden.

Software-Upgrade

Hinweis: PGP Desktop für Mac OS X und PGP Universal Satellite für Mac OS X können nicht gleichzeitig auf demselben System installiert sein. Die Installationsprogramme beider Produkte erkennen, ob das jeweils andere Programm installiert ist, und brechen den Installationsvorgang bei Bedarf ab.

Sie können von einer vorherigen Version der folgenden Produkte ein Upgrade auf PGP Desktop für Mac OS X durchführen:

- PGP Desktop für Mac OS X
- PGP Universal Satellite für Mac OS X

Wichtiger Hinweis: Wenn Sie Ihren Computer auf eine neue Betriebssystemversion aktualisieren und diese Version von PGP Desktop verwenden möchten, deinstallieren Sie zunächst alle älteren Versionen von PGP Desktop, bevor Sie das Betriebssystem aktualisieren und diese Version installieren. Sichern Sie vor der Deinstallation Ihre Schlüssel und Schlüsselbunde. Sollten Sie PGP Whole Disk Encryption verwendet haben, müssen Sie zunächst das Laufwerk entschlüsseln. Erst dann können Sie PGP Desktop deinstallieren.

Upgrade von PGP Desktop durchführen

Führen Sie einen der folgenden Schritte aus:

- **Upgrade von PGP Desktop 8.x oder 9.x für Mac OS X**: Beginnen Sie mit der Installation von PGP Desktop 10.1 für Mac OS X.

  Die vorhandene Version von PGP Desktop für Mac OS X wird automatisch deinstalliert und PGP Desktop 10.1 für Mac OS X wird installiert. Bestehende Schlüsselbunde sowie PGP Virtual Disk-Dateien können in der aktualisierten Version verwendet werden.

- **Upgrade von einer Version von PGP Desktop für Mac OS X vor Version 8.0**: Deinstallieren Sie die vorhandene Software vor der Installation von PGP Desktop 10.1 für Mac OS X. Bestehende Schlüsselbunde sowie PGP Virtual Disk-Dateien können in der aktualisierten Version verwendet werden.

Upgrade von PGP Universal Satellite durchführen

Führen Sie einen der folgenden Schritte aus:

- **Upgrade von PGP Universal Satellite Version 1.2 oder früher für Mac OS X**: Beginnen Sie mit der Installation von PGP Desktop 10.1 für Mac OS X.

  Bestehende Versionen von PGP Universal Satellite für Mac OS X werden automatisch deinstalliert und PGP Desktop 10.1 für Mac OS X wird installiert. Bestehende Einstellungen bleiben erhalten.

  Achtung: Die Installation einer beliebigen Version von PGP Universal Satellite zusätzlich zu PGP Desktop 10.1 für Mac OS X wird nicht unterstützt. Keines der Programme wird in diesem Fall ordnungsgemäß funktionieren. Deinstallieren Sie beide Programme und installieren Sie dann ausschließlich PGP Desktop neu.

- **Upgrade von PGP Desktop für Mac OS X (Version 8.x) und PGP Universal Satellite**: Führen Sie den regulären Installationsvorgang für PGP Desktop 10.1 für Mac OS X aus.

PGP Desktop für Mac OS X und PGP Universal Satellite für Mac OS X werden beide automatisch deinstalliert und PGP Desktop 10.1 für Mac OS X wird installiert. Bestehende Schlüsselbunde und PGP Virtual Disk-Dateien sowie vorhandene Einstellungen für PGP Universal Satellite für Mac OS X können in der aktualisierten Version verwendet werden.

Auf Aktualisierungen prüfen

Hinweis: Die Option zum automatischen Prüfen auf Aktualisierungen ist ab PGP Desktop 10.1 nicht mehr verfügbar. Wenn Sie nach einer Aktualisierung suchen oder eine Aktualisierung installieren möchten, müssen Sie die Datei manuell herunterladen.

Als Folge des Erwerbs der PGP Corporation durch die Symantec Corporation werden die PGP-Abläufe derzeit in die Symantec-Abläufe integriert. Wenn Sie prüfen, ob Aktualisierungen verfügbar sind, oder wenn Sie eine Aktualisierung herunterladen, wählen Sie den zweiten Downloadlink aus, falls der erste Link nicht zu funktionieren scheint.

Gehen Sie folgendermaßen vor, um ein Upgrade für PGP Desktop durchzuführen:

- Rufen Sie das PGP-LEMS (PGP License and Entitlement Management System) auf und melden Sie sich an (https://lems.pgp.com/account/login). Wenn die Aktualisierung für PGP Desktop nicht verfügbar ist, gehen Sie folgendermaßen vor:
- Rufen Sie Symantec FileConnect (https://fileconnect.symantec.com/) auf, wählen Sie die Sprache aus, und geben Sie die Seriennummer ein.

Upgrade von eigenständigen zu verwalteten Installationen von PGP Desktop

Wenn Sie PGP Desktop bisher als eigenständiges Produkt genutzt haben und nun von einem PGP Universal Server verwaltet werden, müssen Sie eine gebundene und gekennzeichnete Version von PGP Desktop auf der vorhandenen eigenständigen Version installieren. Darüber hinaus müssen Sie den Anmeldungsvorgang abschließen. Der PGP-Administrator stellt Ihnen eine Installationsdatei bereit, mit der Sie eine gebundene und gekennzeichnete Version installieren können.

Software des Betriebssystems aktualisieren

Wenn Sie den Computer auf eine neue Major Release des Betriebssystems aktualisieren (z. B. unter Windows auf Windows Vista oder unter Mac OS X von 10.4.x auf 10.5.x), müssen Sie folgende Schritte ausführen:

1 Sichern Sie vor der Deinstallation Ihre Schlüssel und Schlüsselbunde.

2 Sollten Sie PGP Whole Disk Encryption verwendet haben, müssen Sie zunächst das Laufwerk entschlüsseln. Erst dann können Sie PGP Desktop deinstallieren.

3 Deinstallieren Sie alle vorherigen Versionen von PGP Desktop, *bevor* Sie auf die neue Version des Betriebssystems aktualisieren.

4 Nach der Aktualisierung des Betriebssystems können Sie PGP Desktop neu installieren. Importieren Sie Ihre Schlüssel und Ihren Schlüsselbund und verschlüsseln Sie das Laufwerk dann bei Bedarf.

Lizenzierung von PGP Desktop

Lizenzinformationen für diese Version finden Sie in den *Versionshinweisen zu PGP Desktop.*

Einrichtungsassistenten ausführen

Der Einrichtungsassistent zeigt mehrere Bildschirme mit Fragen an. Ihre Antworten werden zur Konfiguration von PGP Desktop verwendet.

Wenn Sie Fragen bezüglich des Einrichtungsassistenten haben, klicken Sie im entsprechenden Fenster des Assistenten auf **Hilfe**.

Mit dem Einrichtungsassistenten werden nicht alle PGP Desktop-Einstellungen konfiguriert. Wenn Sie den Einrichtungsassistenten abgeschlossen haben, können Sie die Einstellungen konfigurieren, die nicht vom Einrichtungsassistenten abgedeckt werden.

Integration mit Entourage 2008

Das Installationspaket von PGP Desktop für Mac OS X enthält Skripte, damit Sie PGP Desktop mit Entourage integrieren können. Nachdem die Skripte in die entsprechenden Ordner kopiert wurden, enthält das Skripte-Menü in Entourage eine PGP-Menüoption. Verschlüsseln Sie mit Entourage-Skripten E-Mail-Texte, ohne einen E-Mail-Proxy verwenden zu müssen.

So integrieren Sie PGP-Skripte mit Entourage

1 Beenden Sie Entourage, falls die Anwendung geöffnet ist.

2 Öffnen Sie den Download von PGP Desktop für Mac OS X.

3 Öffnen Sie im Downloadordner von PGP Desktop den Ordner „Extras“.

4 Öffnen Sie im Ordner „Extras“ den Entourage-Ordner.

5 Doppelklicken Sie auf die Datei `EntourageScripts.zip`, um die folgenden Skripte aus der Zip-Datei zu extrahieren:

- Decrypt & Verify\mod

- Encrypt & Sign\moc
- Encript\moe
- Sign\mos

6 Kopieren Sie die Skripte und fügen Sie sie in den folgenden Ordner ein:

- User Profile\Documents\Microsoft User Data\Entourage Script Menu items\PGP (der Pfad kann bei Ihnen anders lauten)

7 Starten Sie Entourage. Das Skripte-Menü enthält jetzt eine PGP-Menüoption.

Weitere Informationen zum Verschlüsseln und Entschlüsseln von Nachrichten finden Sie unter *PGP-Skripte mit Entourage 2008 verwenden* (auf Seite 137).

Option zum Deinstallieren von PGP Desktop

So deinstallieren Sie PGP Desktop

1 Wählen Sie in PGP Desktop im Menü **PGP** die Option **Deinstallieren** aus. Ein Bestätigungsdialogfeld wird angezeigt.

2 Klicken Sie auf **Ja**, um mit der Deinstallation fortzufahren.

3 Sie werden aufgefordert, sich als administrativer Benutzer des Mac OS X-Systems zu authentifizieren, von dem Sie PGP Desktop deinstallieren möchten. Geben Sie das entsprechende Kennwort ein und klicken Sie auf **OK**. PGP Desktop wird vom System entfernt.

Ihr Schlüsselbund und Ihre PGP Virtual Disk-Dateien werden nicht vom System entfernt, falls Sie PGP Desktop zu einem späteren Zeitpunkt erneut installieren möchten.

PGP Desktop-Installation von einem Computer auf einen anderen übertragen

Es ist nicht schwierig, eine PGP Desktop-Installation von einem Computer auf einen anderen zu übertragen, jedoch müssen einige wichtige Schritte erfolgreich ausgeführt werden. Der Vorgang umfasst folgende Schritte:

So übertragen Sie eine PGP Desktop-Installation auf einen anderen Computer

1 Deinstallieren Sie PGP Desktop. Wählen Sie dazu in PGP Desktop im Menü **PGP** die Option **Deinstallieren** aus.

Beachten Sie, dass mit diesem Schritt die Schlüsselbunddateien nicht gelöscht werden.

2 Übertragen Sie die Schlüsselbunde. Kopieren Sie dazu die Schlüsselbunddateien (sowohl `pubring.pkr` als auch `secring.skr`) vom alten Computer auf einen Wechseldatenträger (z. B. ein Flash-Laufwerk) und dann auf den neuen Computer. Der Standardspeicherort für die Schlüsselbunddateien ist der PGP-Ordner.

   Wenn PGP Desktop zuvor noch nicht auf dem neuen Computer installiert war, müssen Sie diesen Ordner erst erstellen, bevor Sie die Schlüsselbunddateien auf den Computer kopieren.

3 Installieren Sie PGP Desktop auf dem neuen Computer. Laden Sie PGP Desktop hierzu über den Downloadlink aus der E-Mail-Nachricht mit der Auftragsbestätigung herunter.

4 Führen Sie während des Installationsvorgangs folgende Schritte aus:

   - Geben Sie auf dem neuen Computer im Einrichtungsassistenten von PGP Desktop an, dass bereits Schlüsselbunde vorhanden sind**. Führen Sie den Speicherort auf dem neuen Computer auf, an den Sie die Schlüsselbunddateien kopiert haben.**
   - Verwenden Sie dieselben Angaben für Name, Organisation und Lizenznummer, die bei der ursprünglichen Autorisierung von PGP Desktop verwendet wurden.

4 Benutzeroberfläche von PGP Desktop

In diesem Abschnitt wird die Benutzeroberfläche von PGP Desktop beschrieben.

In diesem Kapitel

Auf PGP Desktop-Funktionen zugreifen 27
Notifier-Warnungen von PGP Desktop 32
PGP Desktop und der Finder 39
PGP-Protokoll anzeigen 46

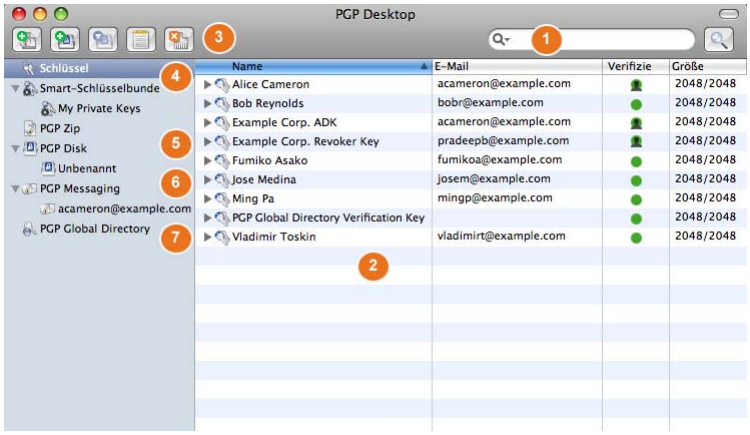
Auf PGP Desktop-Funktionen zugreifen

Es gibt vier grundlegende Möglichkeiten, auf PGP Desktop zuzugreifen:

- *Hauptbildschirm von PGP Desktop* (auf Seite 28)
- *PGP Desktop-Symbol in der Menüleiste verwenden* (auf Seite 29)
- *PGP-Dock-Symbol verwenden* (auf Seite 30)
- *Finder von Mac OS X verwenden* (auf Seite 32)

Hauptbildschirm von PGP Desktop

Der Hauptbildschirm von PGP Desktop stellt die primäre Schnittstelle zum Produkt dar.



Der Hauptbildschirm von PGP Desktop enthält Folgendes:

1	**Suchfeld**: Ermöglicht die Suche nach Schlüsseln am lokalen Schlüsselbund. Geben Sie einfach eine Zeichenfolge ein und die Namen und E-Mail-Adressen am lokalen Schlüsselbund, die diese Zeichenfolge enthalten, werden angezeigt. Klicken Sie auf **Erweiterte Suche**, um weitere Suchkriterien einzublenden.
2	**Arbeitsbereich von PGP Desktop**: Zeigt Informationen an sowie Aktionen, die für das ausgewählte Element durchgeführt werden können.
3	**Symbolleiste**: Ermöglicht den Zugriff auf häufig genutzte Funktionen. Sie haben folgende Möglichkeiten: Ein neues PGP Zip-Archiv erstellen Ein neues PGP Virtual Disk-Laufwerk erstellen Ein vorhandenes PGP Virtual Disk-Laufwerk aktivieren Schlüssel synchronisieren Dateien sicher löschen
4	**Symbol für Schlüssel**: Ermöglicht Ihnen, die von PGP Desktop verwalteten PGP-Schlüssel zu kontrollieren.
5	**Symbol für PGP Disk**: Ermöglicht Ihnen, PGP Virtual Disk-Laufwerke anzuzeigen und zu verwalten. Zudem können Sie neue PGP Virtual Disk-Laufwerke erstellen und ein Laufwerk, das nicht zum Starten verwendet wird, mit PGP Whole Disk Encryption vollständig

	verschlüsseln.
6	**Symbol für PGP Messaging**: Ermöglicht Ihnen, die PGP Messaging-Dienste zu verwalten. Darüber hinaus können Sie neue Dienste und Richtlinien erstellen sowie die vorhandenen Dienste und Richtlinien verwalten.
7	**Symbol für Keyserver**: Ermöglicht Ihnen, Keyserver anzuzeigen und zu verwalten.
	(nicht abgebildet) **Symbol für PGP Zip:** Ermöglicht Ihnen, PGP Zip-Archive anzuzeigen und zu verwalten.

PGP Desktop-Symbol in der Menüleiste verwenden

Eine Möglichkeit, auf viele der Funktionen von PGP Desktop zuzugreifen, ist das PGP Desktop-Symbol in der Menüleiste.

Wenn Sie auf das PGP Desktop-Symbol in der Menüleiste klicken, wird das PGP-Menü angezeigt. Möglicherweise sind nicht alle Optionen verfügbar. Dies ist davon abhängig, ob Sie eine eigenständige oder eine verwaltete Installation verwenden.

- **Info über PGP Desktop**: Zeigt ein Fenster mit der verwendeten PGP Desktop-Version, den Lizenzinformationen sowie eine Liste der an der Entwicklung von PGP Desktop beteiligten Personen an. Darüber hinaus weist dieses Fenster eine Schaltfläche auf, über die Sie PGP Desktop deinstallieren können.
- **Hilfe**: Öffnet die integrierte Online-Hilfe von PGP Desktop.
- **PGP Desktop öffnen: Öffnet den Hauptbildschirm von PGP Desktop.**
- **PGP Viewer öffnen**: Öffnet PGP Viewer, sodass Sie E-Mail-Nachrichten außerhalb des E-Mail-Stroms entschlüsseln können.
- **Notifier anzeigen**: Öffnet das Notifier-Fenster von PGP Desktop, in dem Sie die angezeigten Notifier-Meldungen überprüfen können.
- **Protokoll anzeigen: Zeigt das PGP Desktop-Protokoll an. Das PGP Desktop-Protokoll gibt Aufschluss darüber, welche Aktionen von PGP Desktop ausgeführt werden, um Ihre Daten zu schützen.**
- **Protokoll löschen: Löscht das PGP-Protokoll.**
- **Richtlinie aktualisieren**: Eine Richtlinie wird manuell vom PGP Universal Server heruntergeladen. Diese Option steht nur bei verwalteten Installationen zur Verfügung.

- **Passphrase ändern**: Ermöglicht Ihnen das Ändern der Passphrase Ihres Schlüssels. Diese Option steht nur bei verwalteten Installationen zur Verfügung.
- **Caches leeren: Entfernt alle zwischengespeicherten Daten, z. B. Passphrasen und zwischengespeicherte öffentliche Schlüssel, aus dem Arbeitsspeicher des Computers.**
- **Ausblenden: Entfernt das PGP-Symbol aus der Menüleiste. Die Hintergrundkomponenten der Anwendung bleiben jedoch aktiv.**

  Wenn Sie beim Klicken auf das PGP Desktop-Symbol die **Wahltaste** gedrückt halten, wird der Befehl **Ausblenden** durch den Befehl **Beenden** ersetzt. Das PGP Desktop-Symbol wird dadurch aus der Menüleiste entfernt und die *Hintergrundkomponenten von PGP Desktop werden beendet*. Das Kontextmenü funktioniert weiterhin.

Achtung: Wenn Sie die Hintergrundkomponenten von PGP Desktop mithilfe der Wahltaste und des PGP-Symbols in der Menüleiste beenden, werden E-Mail-Nachrichten nicht mehr verschlüsselt, entschlüsselt, signiert oder verifiziert. Nachrichten, die Sie empfangen haben, während die Hintergrundkomponenten von PGP Desktop nicht ausgeführt wurden, können möglicherweise sogar nach einem Neustart der Komponenten nicht entschlüsselt werden. Darüber hinaus findet ohne aktive Hintergrundkomponenten der Software keine Schlüsselverwaltung statt. Aus diesen Gründen sollten die Hintergrundprozesse von PGP Desktop nie deaktiviert werden.

So starten Sie die Hintergrundprozesse von PGP Desktop neu, wenn die Anwendung nicht ausgeführt wird

1. Suchen Sie auf dem System nach PGP Desktop. Der Standardspeicherort ist der Ordner „Programme“.
2. Doppelklicken Sie auf das Symbol der PGP Desktop-Anwendung. PGP Desktop wird gestartet und das Symbol wird in der Menüleiste angezeigt.

PGP-Dock-Symbol verwenden

Eine Möglichkeit, auf viele der Funktionen von PGP Desktop zuzugreifen, ist das PGP-Dock-Symbol.

Nutzen Sie eine dieser Möglichkeiten zum Verwenden des Menüs des PGP Desktop-Symbols im Dock von Mac OS X und wählen Sie anschließend eine Option aus dem angezeigten Menü aus:

- Klicken Sie auf das PGP Desktop-Dock-Symbol und halten Sie die Maustaste gedrückt.

- Halten Sie die Ctrl-Taste gedrückt und klicken Sie auf das Dock-Symbol.
- Klicken Sie mit der rechten Maustaste auf das Dock-Symbol, wenn Sie eine Maus mit zwei Tasten verwenden.

Das PGP Desktop-Symbol wird im Dock angezeigt, wenn die Anwendung geöffnet ist oder wenn Sie das PGP Desktop-Symbol manuell im Dock platziert haben.

Wenn die Anwendung geöffnet ist und Sie auf das PGP Desktop-Symbol im Dock klicken und die *Maustaste gedrückt halten* (oder bei gedrückter Ctrl-Taste bzw. bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste klicken), wird ein Menü mit folgenden Optionen angezeigt:

- Alle derzeit geöffneten PGP Desktop-Fenster: Wenn PGP Desktop ausgeführt wird, werden die aktuell geöffneten Fenster oben in diesem Menü angezeigt.
- **Info über PGP Desktop**: Zeigt das Dialogfeld mit Informationen zu PGP Desktop an. In diesem Dialogfeld werden eine Liste der an der Entwicklung von PGP Desktop beteiligten Personen sowie Informationen über die von Ihnen verwendete Version angezeigt. Darüber hinaus weist es eine Schaltfläche auf, über die Sie PGP Desktop deinstallieren können.
- **Einstellungen**: Öffnet das Dialogfeld mit den PGP Desktop-Einstellungen.
- **Zwischenablage**: Ermöglicht Ihnen, den Inhalt der Zwischenablage zu verschlüsseln, zu signieren, zu verschlüsseln und zu signieren oder zu entschlüsseln und zu verifizieren.
- **Caches leeren**: Entfernt alle zwischengespeicherten Daten, z. B. Passphrasen und zwischengespeicherte öffentliche Schlüssel, aus dem Arbeitsspeicher des Computers.

Bei den verbleibenden Menüelementen im unteren Menüabschnitt handelt es sich um standardmäßige Dockelemente von Mac OS X:

- **Aus dem Dock entfernen/Im Dock behalten: Das PGP Desktop-Symbol wird dem Dock hinzugefügt oder aus diesem entfernt.**
- **Bei der Anmeldung öffnen: Stellt die Mac OS X-Kontoeinstellungen so ein, dass PGP Desktop automatisch gestartet wird, wenn Sie sich am Computer anmelden.**
- **Im Finder anzeigen**: Zeigt den Speicherort von PGP Desktop in einem Finder-Fenster an.
- **Ausblenden**: Blendet eventuell geöffnete PGP Desktop-Fenster aus.
- **Beenden**: Beendet die PGP Desktop-Anwendung.

Wenn Sie auf das PGP Desktop-Symbol im Dock klicken und die Maustaste gedrückt halten, wenn die Anwendung nicht geöffnet ist, werden die standardmäßigen Docksymbole von Mac OS X angezeigt.

Finder von Mac OS X verwenden

Klicken Sie auf dem Schreibtisch oder in einem Finder-Fenster bei gedrückter Ctrl-Taste (bzw. bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste) auf eine Datei oder einen Ordner. Wählen Sie im Kontextmenü die Option **PGP** aus.

Sie können auch über den Finder von Mac OS X auf Funktionen von PGP Desktop zugreifen.

So verwenden Sie den Finder von Mac OS X

1. Öffnen Sie ein Finder-Fenster.
2. Klicken Sie bei gedrückter Ctrl-Taste (oder klicken Sie bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste) auf die gewünschte Datei bzw. den gewünschten Ordner.
3. Wählen Sie die entsprechende Option im PGP-Kontextmenü aus. Wählen Sie **Verschlüsseln**, **Signieren**, **Verschlüsseln und signieren**, **Entschlüsseln/Verifizieren**, **Sicher löschen** oder **Aktivieren** aus (falls Sie PGP Virtual Disk-Laufwerke verwenden).

Tipp: Sie können auch auf dem Schreibtisch mit der rechten Maustaste auf eine Datei oder einen Ordner klicken.

Notifier-Warnungen von PGP Desktop

Die Notifier-Funktion von PGP Desktop zeigt in einem kleinen Fenster Informationen zum Status von ein- und ausgehenden E-Mail-Nachrichten sowie zu Instant Messaging-Sitzungen an.

In einer von einem PGP Universal Server verwalteten Umgebung hat der Administrator möglicherweise bestimmte Benachrichtigungseinstellungen festgelegt (z. B. die Anzeige von Benachrichtigungen oder die Position des Notifier-Fensters). In diesem Fall werden möglicherweise keine Notifier-Meldungen angezeigt.

PGP Desktop Notifier für Messaging

PGP Desktop Notifier für Messaging bietet folgende Funktionen:

- Anzeigen von Benachrichtigungen, ob eingehende E-Mail-Nachrichten ordnungsgemäß entschlüsselt und/oder signiert wurden
- Anzeigen von Benachrichtigungen, ob ausgehende E-Mail-Nachrichten ordnungsgemäß verschlüsselt und/oder signiert werden

- Verhindern des Sendens von E-Mail-Nachrichten, wenn die Verschlüsselungsoptionen nicht Ihren Wünschen entsprechen
- Anzeigen einer kurzen Übersicht mit Absender, Betreff und Verschlüsselungsschlüssel einer E-Mail-Nachricht
- Überprüfen des Status der in der aktuellen Windows-Sitzung bereits eingegangenen oder ausgegangenen E-Mail-Nachrichten
- Anzeigen von Benachrichtigungen, ob eine Chat-Sitzung mit einem anderen Benutzer von PGP Desktop geschützt wird

Mit der Notifier-Funktion von PGP Desktop können Sie alle oder bestimmte eingehende E-Mail-Nachrichten überwachen sowie das Senden aller oder bestimmter ausgehender E-Mail-Nachrichten genau steuern. Die Entscheidung liegt bei Ihnen. Sie können verschiedene Notifier-Optionen festlegen oder die Notifier-Funktion von PGP Desktop bei Bedarf vollständig deaktivieren.

Beachten Sie bei der Arbeit mit der Notifier-Funktion von PGP Desktop folgende zusätzliche Hinweise:

- Navigieren Sie bei Meldungen zu Nachrichten mit den Pfeilschaltflächen nach links und rechts in der rechten oberen Ecke des Notifier-Fensters vorwärts oder rückwärts durch die Notifier-Meldungen. Auf diese Weise können Sie die Meldungen überprüfen, die vor oder nach der aktuell angezeigten Meldung eingegangen sind.
- Die Notifier-Meldungsfenster werden zunächst teilweise transparent angezeigt, damit der Bildschirminhalt nicht verdeckt wird. Sie werden undurchsichtig angezeigt, wenn Sie mit dem Mauszeiger über das Fenster fahren, und werden wieder transparent, wenn Sie den Mauszeiger aus dem Meldungsfenster entfernen.
- Sofern der Mauszeiger nicht über einer Notifier-Meldung platziert ist, wird diese Meldung vier Sekunden lang angezeigt. Diese Standardeinstellung kann in den Notifier-Optionen geändert werden. Wenn Sie mehr Zeit zum Lesen einer Meldung benötigen, zeigen Sie mit dem Mauszeiger auf die Meldung, damit sie eingeblendet bleibt.
- Wenn Sie eine Notifier-Meldung verpassen oder eine ältere Meldung noch einmal ansehen möchten, gehen Sie wie folgt vor:
  - Windows: Klicken Sie im PGP-Symbol im Infobereich der Taskleiste auf **Notifier anzeigen.**
  - Mac OS X: Klicken Sie in der Menüleiste von Mac OS X auf das PGP Desktop-Symbol und wählen Sie **Notifier anzeigen** aus.
- Schließen Sie eine Notifier-Meldung, indem Sie auf das **X** klicken (oben rechts in der Meldung bei Windows-Systemen und oben links bei Mac OS X-Systemen).

Weitere Informationen zum Einrichten der Notifier-Optionen von PGP Desktop finden Sie unter *Notifier-Optionen* (siehe "*Benachrichtigungseinstellungen*" auf Seite 229).

PGP Desktop Notifier-Meldungen zu eingehenden Nachrichten

Meldungen zu eingehenden E-Mail-Nachrichten können Sie entnehmen, ob die E-Mail-Nachricht entschlüsselt und verifiziert wurde oder mit einem nicht verifizierten oder unbekannten Schlüssel entschlüsselt oder signiert wurde.

PGP Desktop Notifier-Meldungen zu ausgehenden Nachrichten

Für eine einfache Benachrichtigung können Sie wählen, dass beim Senden von E-Mail-Nachrichten kurz eine PGP Desktop Notifier-Meldung angezeigt wird. Diese Meldung kann für alle E-Mail-Nachrichten oder nur für bestimmte E-Mail-Nachrichten erfolgen, die bestimmte Kriterien erfüllen. Die Notifier-Meldung zeigt an, dass PGP Desktop nach den öffentlichen Schlüsseln des in der Zeile „An“ aufgeführten Empfängers sucht. Werden die entsprechenden Schlüssel gefunden, ändert sich die Statuszeile und zeigt an, dass die Nachricht verschlüsselt versendet wird. Werden die entsprechenden Schlüssel nicht gefunden, geht PGP Desktop entsprechend der festgelegten Richtlinien vor und sendet die Nachricht unverschlüsselt oder blockiert sie.

Nachdem eine Nachricht verschlüsselt gesendet wurde, klicken Sie auf **Mehr**, um nähere Informationen zur Verarbeitung der Nachricht durch PGP Desktop zu erhalten. Es ist nicht zwingend erforderlich, diese zusätzlichen Informationen anzuzeigen. Klicken Sie zum Ausblenden der zusätzlichen Angaben auf **Weniger**.

Sie können den Versand einer Nachricht verzögern, indem Sie den Mauszeiger auf das Notifier-Fenster bewegen. Sie haben dazu 4 Sekunden Zeit (diese Zeitspanne kann für die Notifier-Funktion unter „Einstellungen“ geändert werden). Danach wird die Nachricht unverschlüsselt gesendet und im Feld „Status“ ein entsprechender Hinweis angezeigt.

Wenn Sie den Mauszeiger nicht auf die Nachricht bewegen, werden im Notifier-Fenster die Schaltflächen **Blockieren** und **Senden** angezeigt. Klicken Sie auf **Blockieren**, um die Übertragung der Nachricht zu stoppen, oder auf **Senden**, um die Nachricht zu senden.

Wenn Sie eine E-Mail-Nachricht an mehrere Empfänger senden und PGP Desktop nur für einen Teil der Empfänger Schlüssel findet, wird in der Notifier-Meldung eine entsprechende Statusmeldung angezeigt. Sie haben in diesem Fall zwei Möglichkeiten:

- Senden Sie die E-Mail-Nachricht an Empfänger mit Schlüsseln verschlüsselt und an Empfänger ohne Schlüssel unverschlüsselt.
- Blockieren Sie die Nachricht, damit Sie an keinen der Empfänger gesendet wird.

PGP Desktop Notifier-Meldungen zu ausgehenden Nachrichten für Offline-Richtlinien

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, hat der Administrator u. U. festgelegt, welche Aktionen bei ausgehenden Nachrichten durchgeführt werden, wenn der PGP Universal Server nicht verfügbar ist. Die Notifier-Meldung zu ausgehenden Nachrichten zeigt Folgendes an:

- Der PGP Universal Server ist nicht verfügbar und per Richtlinie werden alle Nachrichten blockiert. E-Mail-Nachrichten bleiben im Postausgang und werden gesendet, wenn eine Verbindung zum PGP Universal Server hergestellt werden kann.
- Der PGP Universal Server ist nicht verfügbar und per Richtlinie werden alle Nachrichten als Klartext gesendet.
- Der PGP Universal Server ist nicht verfügbar und per Richtlinie wurde einer lokalen Richtlinie Vorrang eingeräumt.

In den letzten beiden Fällen können Sie die ausgehende Nachricht, wie jede andere ausgehende Nachricht, senden oder blockieren.

PGP Notifier für Instant Messaging

Wenn PGP Desktop auf dem Computer installiert ist und Sie die Notifier-Funktion für Instant Messaging aktiviert haben (in den PGP Desktop-Einstellungen auf der Registerkarte **Benachrichtigungen**), werden Sie in Notifier-Meldungen von PGP Desktop darüber informiert, wenn AIM-Sitzungen (AOL Instant Messenger) mit anderen PGP Desktop-Benutzern geschützt sind.

Wenn Sie die Funktion für sicheres Instant Messaging verwenden, wird beim Anmelden im Instant Messaging-Programm eine Notifier-Meldung angezeigt, dass der Chat sicher ist. Zudem wird in den meisten AIM-kompatiblen Instant Messaging-Clients ein Schlosssymbol neben Ihrem Buddy-Namen angezeigt.

Wenn Sie sich vom Instant Messaging-Programm abmelden, werden Sie in einer abschließenden Notifier-Meldung darüber informiert, dass die sichere Sitzung beendet wurde.

Weitere Informationen zur Konfiguration und Verwendung der Funktion für sichere Instant Message-Chats finden Sie unter IM-Nachrichten sichern.

Notifier-Meldungen aktivieren oder deaktivieren

In einer von einem PGP Universal Server verwalteten Umgebung hat der Administrator möglicherweise bestimmte Benachrichtigungseinstellungen festgelegt (z. B. die Anzeige von Benachrichtigungen oder die Position des Notifier-Fensters). In diesem Fall ist im Fenster „Einstellungen“ der Bereich **Benachrichtigungen** nicht verfügbar und wird nicht angezeigt.

So aktivieren oder deaktivieren Sie Notifier-Meldungen

1. Öffnen Sie PGP Desktop und wählen Sie **PGP > Einstellungen** aus.
2. Klicken Sie auf das Symbol „Notifier".
3. Wählen Sie unter **Verwendung** die Option **PGP Notifier verwenden** aus, wenn Sie die Funktion aktivieren möchten, und legen Sie den Speicherort fest. PGP Desktop-Benachrichtigungen können in einer der vier Ecken des Bildschirms angezeigt werden (**Unten rechts**, **Unten links**, **Oben rechts** oder **Oben links**). Wählen Sie die Ecke aus, in der die PGP Desktop-Benachrichtigungen angezeigt werden sollen. Die Standardposition ist **Oben links**.
4. Wenn Sie PGP Desktop Messaging verwenden und die Notifier-Meldungen von PGP Desktop eingeblendet werden sollen, in denen der Verschlüsselungs- oder Signierstatus beim Senden von E-Mail-Nachrichten angezeigt wird, aktivieren Sie das Kontrollkästchen **Beim Verarbeiten ausgehender E-Mail-Nachrichten benachrichtigen**. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie beim Senden von E-Mail-Nachrichten keine PGP Desktop-Benachrichtigungen wünschen.
5. PGP Desktop sucht nach einem öffentlichen Schlüssel für jeden Empfänger der von Ihnen gesendeten E-Mail-Nachrichten. Wenn für einen Empfänger kein öffentlicher Schlüssel gefunden werden kann, wird die betreffende E-Mail-Nachricht standardmäßig als Klartext (ohne Verschlüsselung) gesendet. Wählen Sie die Option **Vor dem Senden von E-Mail-Nachrichten nachfragen, wenn der Schlüssel des Empfängers nicht gefunden wird** aus, wenn Sie informiert werden möchten, wenn ein Schlüssel nicht gefunden wird. Sie erhalten dann die Möglichkeit, die E-Mail-Nachricht zu blockieren, sodass sie nicht gesendet wird. Legen Sie dann folgende Optionen fest:

   - **Vor dem Senden von E-Mail-Nachrichten immer nachfragen:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie jede E-Mail-Nachricht vor dem Versand bestätigen möchten. Sie können den Verschlüsselungsstatus im Notifier-Fenster überprüfen und dann entscheiden, ob die E-Mail-Nachricht gesendet oder blockiert werden soll.
   - **Ausgehende E-Mail-Nachricht zum Bestätigen um n Sekunden verzögern** (wobei *n* für eine Zahl zwischen 1 und 30 steht; der Standardwert beträgt 4 Sekunden): Ändern Sie die Verzögerungszeit für ausgehende Nachrichten sowie die Zeit für die Anzeige des Notifier-Fensters von PGP Desktop, indem Sie die Pfeiltasten nach oben und nach unten verwenden. Innerhalb der Verzögerungszeit können Sie die Notifier-Meldung von PGP Desktop überprüfen.

   (Weitere Informationen zu den Einstellungen für die Standardrichtlinien von PGP Desktop finden Sie unter *Dienste und Richtlinien* (auf Seite 103).)

6 Geben Sie für eingehende E-Mail-Nachrichten an, wie deren Status beim Empfang angezeigt werden soll. Wählen Sie unter **Benachrichtigungen für eingehende E-Mail-Nachrichten anzeigen** eine der folgenden Optionen aus:

- **Beim Empfang sicherer E-Mail-Nachrichten**: Beim Empfang sicherer E-Mail-Nachrichten wird ein Notifier-Fenster angezeigt. Dieses Fenster enthält den Absender der E-Mail-Nachricht, den Betreff, den Verschlüsselungs- sowie den Verifizierungsstatus und die E-Mail-Adresse des Absenders.
- **Nur beim Fehlschlagen der Nachrichtenüberprüfung**: Eine Notifier-Meldung wird nur dann für eingehende E-Mail-Nachrichten angezeigt, wenn PGP Desktop die Signatur der eingehenden E-Mail-Nachricht nicht verifizieren kann.
- **Nie**: Wählen Sie diese Option aus, wenn beim Empfang von E-Mail-Nachrichten keine Notifier-Meldung angezeigt werden soll. Diese Option wirkt sich nicht auf Notifier-Meldungen für ausgehende E-Mail-Nachrichten aus.

7 Wenn zu Beginn und bei Beendigung eines sicheren Instant Messaging-Chats kurz eine Notifier-Meldung von PGP Desktop angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Über Status verschlüsselter PGP-IM-Sitzungen benachrichtigen**.

5

PGP Desktop und der Finder

In diesem Abschnitt wird beschrieben, wie Sie mithilfe der Kontextmenüs im Finder auf bestimmte Funktionen von PGP Desktop zugreifen können.

In diesem Kapitel

Übersicht 39
Verschlüsseln, signieren oder verschlüsseln und signieren 40
Sicher löschen 42
Entschlüsseln/Verifizieren 42
PGP Virtual Disk-Laufwerke aktivieren oder deaktivieren 43
PGP-Schlüssel importieren 44
Öffentliche PGP-Schlüssel zum Schlüsselbund hinzufügen 45
Inhalt von PGP Zip-Archiven extrahieren 45

Übersicht

Über die Kontextmenüs im Finder können Sie auf die gleichen PGP Desktop-Funktionen zugreifen wie über das Dienste-Menü von Mac OS X.

Abhängig von der jeweiligen Auswahl haben Sie folgende Möglichkeiten:

- Verschlüsseln, signieren oder verschlüsseln und signieren
- Sicher löschen
- Entschlüsseln und verifizieren
- PGP Virtual Disk-Laufwerke aktivieren, bearbeiten oder deaktivieren
- PGP-Schlüssel importieren
- PGP-Schlüssel dem Schlüsselbund hinzufügen

Inhalte von PGP Zip-Archiven anzeigen Greifen Sie folgendermaßen auf Kontextmenüs im Finder zu:

- Ctrl+Klicken: Bei einer Maus mit einer Taste halten Sie auf der Tastatur die Ctrl-Taste gedrückt und klicken auf das Objekt.

- Klicken mit der rechten Maustaste: Bei einer Maus mit zwei Tasten klicken Sie mit der rechten Maustaste auf das Objekt.

In diesem Dokument wird das Klicken bei gedrückter Ctrl-Taste verwendet. Wenn Sie mit der rechten Maustaste klicken oder eine andere Methode für den Zugriff auf die Kontextmenüs im Finder verwenden, ersetzen Sie das Klicken bei gedrückter Ctrl-Taste durch Ihre eigene Methode.

Hinweis: Zu den Dateien im Finder gehören für diese Zwecke auch die Dateien auf dem Schreibtisch von Mac OS X.

Verschlüsseln, signieren oder verschlüsseln und signieren

Mit PGP Desktop können Sie Dateien, Ordner und sogar ganze Laufwerke über den Finder verschlüsseln, signieren oder verschlüsseln und signieren.

Das Verschlüsseln und/oder Signieren von Dateien und Ordnern bietet sich an, um nur ein paar wichtige Dateien und/oder Ordner zu schützen, wenn sich die Verwendung eines PGP Virtual Disk-Laufwerks nicht lohnt.

Wenn Sie in Betracht ziehen, ein Laufwerk im Finder zu verschlüsseln und/oder zu signieren, ist ein PGP Virtual Disk-Laufwerk möglicherweise die bessere Lösung. Weitere Informationen finden Sie unter PGP Virtual Disk-Laufwerke verwenden.

So verschlüsseln und/oder signieren Sie Dateien und/oder Ordner im Finder

1. Wählen Sie im Finder die Dateien und/oder Ordner aus, die Sie verschlüsseln und/oder signieren möchten. Mithilfe der Umschalt- oder Befehlstaste können Sie beliebige Kombinationen von Dateien und Ordnern auswählen.
2. Klicken Sie bei gedrückter Ctrl-Taste auf die ausgewählten Dateien und/oder Ordner oder klicken Sie bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste darauf. Wählen Sie aus dem Kontextmenü aus dem Menü **PGP** die Option **Verschlüsseln und signieren** **aus. (Falls Sie nur** **Verschlüsseln** auswählen, werden Sie *nicht* aufgefordert, einen Signaturschlüssel anzugeben. Falls Sie nur **Signieren** auswählen, werden Sie *nicht* aufgefordert, einen öffentlichen Schlüssel zum Verschlüsseln auszuwählen.) Das Dialogfeld „PGP-Empfänger“ wird angezeigt.
3. Ziehen Sie die öffentlichen Schlüssel der Personen, die die von Ihnen verschlüsselten Objekte entschlüsseln sollen, unten im Dialogfeld in das Feld **Empfänger**.
4. Klicken Sie oberhalb der Schaltfläche **OK** auf das Symbol mit dem Pfeil nach unten, um die gewünschten Optionen festzulegen:

- **Konventionelle Verschlüsselung**: Aktivieren Sie dieses Kontrollkästchen, wenn Sie sich auf eine allgemeine Passphrase anstatt auf die Kryptografie mit einem öffentlichen Schlüssel verlassen möchten. Die Datei wird mit einem Sitzungsschlüssel verschlüsselt, der die Verschlüsselung (und Entschlüsselung) mit einer von Ihnen angegebenen Passphrase ausführt.

  Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist die konventionelle Verschlüsselung möglicherweise deaktiviert.

- **Textausgabe**: Bei einigen E-Mail-Anwendungen müssen Sie beim Versenden von Dateien als Anlage das Kontrollkästchen **Textausgabe** aktivieren, um die Datei als ASCII-Text zu speichern. Dies ist in einigen Fällen erforderlich, um eine binäre Datei mit älteren E-Mail-Anwendungen zu senden. Wenn Sie diese Option auswählen, nimmt die Größe der verschlüsselten Datei um ca. 30 Prozent zu.

- **Original sicher löschen**: Aktivieren Sie diese Option, um das Originaldokument zu überschreiben, das Sie verschlüsseln. Ihre vertraulichen Daten können dann nicht von Personen gelesen werden, die Zugriff auf das System haben.

- **MacBinary**: MacBinary ist die Standardmethode, mit der eine Mac OS X-Datei in eine einzelne Datei umgewandelt wird, die dann ohne Verlust des Daten- oder Ressourcensegments auf einen Macintosh oder PC übertragen werden kann. Die verfügbaren Optionen sind „Ja“, „Nein“ und „Smart“.

  Bei **Ja** wird die gesamte Datei eingeschlossen, einschließlich der für Mac OS X spezifischen Daten. Bei **Nein** wird nur das Datensegment eingeschlossen. Bei **Smart** hängt es vom Dateityp ab, ob die für Mac OS X spezifischen Daten eingeschlossen werden.

5. Klicken Sie auf **OK**. Wenn Sie die konventionelle Verschlüsselung ausgewählt haben, werden Sie aufgefordert, eine Passphrase zum Schutz der verschlüsselten Objekte einzugeben.
6. Geben Sie eine Passphrase ein. Wiederholen Sie die Eingabe und klicken Sie auf **OK**. Das Dialogfeld „PGP-Passphrase eingeben“ wird angezeigt.
7. Geben Sie mithilfe der Liste „Signaturschlüssel“ einen privaten Schlüssel an, der zum Signieren der von Ihnen verschlüsselten und signierten Objekte dienen soll. Geben Sie anschließend die Passphrase des Signaturschlüssels ein. Falls die Passphrase zwischengespeichert wurde, ist eine erneute Eingabe nicht erforderlich.

   Als zusätzliche Sicherheitsmaßnahme werden die für die Passphrase eingegebenen Zeichen in der Regel nicht auf dem Bildschirm angezeigt. Falls Sie jedoch sicher sind, dass Ihnen niemand zusieht (weder physisch noch über das Netzwerk), und wenn Sie die Zeichen der Passphrase beim Eingeben sehen möchten, aktivieren Sie das Kontrollkästchen **Tastatureingabe anzeigen**.

8 Wenn die Passphrase im Mac OS X-Schlüsselanhänger gespeichert werden soll, aktivieren Sie das entsprechende Kontrollkästchen. Sie müssen die Passphrase dann beim nächsten Zugriff auf diese Funktion nicht erneut eingeben.

9 Klicken Sie auf **OK**. Am Speicherort der verschlüsselten und signierten Objekte wird ein PGP Zip-Archiv (<Dateiname>.pgp) erstellt.

Sicher löschen

In Situationen, in denen Sie absolut sicher sein möchten, dass bestimmte Dateien und/oder Ordner vom System gelöscht wurden, können Sie die Objekte über den Finder sicher löschen.

Wenn Sie eine Datei oder einen Ordner in den Papierkorb von Mac OS X verschieben, bedeutet dies lediglich, dass diese Dateien oder Ordner, von denen Sie annehmen, dass sie „gelöscht“ werden, von neuen Dateien überschrieben werden können. Tatsächlich könnten alle Personen mit physischem Zugriff auf das System diese Dateien über mehrere Tage, Wochen oder sogar Monate abrufen.

Mit PGP Desktop Shred werden die Dateien hingegen mehrmals überschrieben, wenn sie von Ihnen sicher gelöscht werden. Weitere Informationen zur Effizienz der Funktion zum sicheren Löschen finden Sie unter Dateien sicher löschen.

So werden Dateien und/oder Ordner im Finder sicher gelöscht

1 Wählen Sie im Finder die Dateien und/oder Ordner aus, die Sie sicher löschen möchten. Mithilfe der Umschalt- oder Befehlstaste können Sie beliebige Kombinationen von Dateien und Ordnern auswählen.

2 Klicken Sie bei gedrückter Ctrl-Taste auf die ausgewählten Dateien und/oder Ordner oder klicken Sie bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste darauf.

3 Wählen Sie im Kontextmenü die Option **PGP** und dann die Option **Sicher löschen** aus. In einem PGP-Bildschirm werden Sie aufgefordert, das sichere Löschen der aufgeführten Dateien zu bestätigen.

4 Klicken Sie auf **OK**. Die Dateien werden sicher vom System gelöscht und werden auch im Papierkorb nicht angezeigt.

Entschlüsseln/Verifizieren

Falls auf dem System eine PGP Zip-Datei (.pgp) vorhanden ist, können Sie diese im Finder entschlüsseln und verifizieren. Mit „Entschlüsseln/Verifizieren“ werden verschlüsselte Dateien (.pgp) immer entschlüsselt. Wenn die verschlüsselte Datei jedoch nicht signiert war, wird sie auch nicht verifiziert (da keine Signatur vorhanden ist).

Sie können auch PGP-Schlüsseldateien (`.asc`) entschlüsseln/verifizieren, jedoch dient dieser Vorgang nur zum Importieren der Schlüssel und nicht zum Entschlüsseln oder Verifizieren der Datei. Weitere Informationen zum Importieren von PGP-Schlüsseln aus einer ASC-Datei im Finder finden Sie unter *PGP-Schlüssel importieren* (auf Seite 44).

So entschlüsseln/verifizieren Sie eine PGP Zip-Datei im Finder

1. Wählen Sie im Finder die PGP Zip-Datei (`.pgp`) aus, die Sie entschlüsseln/verifizieren möchten.
2. Klicken Sie bei gedrückter Ctrl-Taste auf die ausgewählten Dateien und/oder Ordner oder klicken Sie bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste darauf. Wählen Sie im Kontextmenü die Option **PGP** und dann die Option **Entschlüsseln und verifizieren** aus. Das Dialogfeld „PGP-Passphrase eingeben“ wird angezeigt.
3. Geben Sie die entsprechende Passphrase für den privaten Schlüssel ein. Falls die Passphrase zwischengespeichert wurde, werden Sie nicht zur Eingabe aufgefordert.

   Als zusätzliche Sicherheitsmaßnahme werden die für die Passphrase eingegebenen Zeichen in der Regel nicht auf dem Bildschirm angezeigt. Falls Sie jedoch sicher sind, dass Ihnen niemand zusieht (weder physisch noch über das Netzwerk), und wenn Sie die Zeichen der Passphrase beim Eingeben sehen möchten, aktivieren Sie das Kontrollkästchen **Tastatureingabe anzeigen**.
4. Wenn die Passphrase im Mac OS X-Schlüsselanhänger gespeichert werden soll, aktivieren Sie das entsprechende Kontrollkästchen. Sie müssen die Passphrase dann beim nächsten Zugriff auf diese Funktion nicht erneut eingeben.
5. Klicken Sie auf **OK**. Die Datei wird am Speicherort der PGP-Datei entschlüsselt. Wenn die Datei signiert wurde, zeigt PGP Desktop im Fenster „Verifizierungsinformationen“ das Ergebnis der Verifizierung an.

PGP Virtual Disk-Laufwerke aktivieren oder deaktivieren

Wenn Sie über eine deaktivierte PGP Virtual Disk-Datei (.pgd) verfügen, können Sie das entsprechende PGP Virtual Disk-Laufwerk über den Finder aktivieren. Weitere Informationen zu PGP Virtual Disk-Laufwerken finden Sie unter PGP Virtual Disk-Laufwerke verwenden.

So aktivieren Sie ein PGP Virtual Disk-Laufwerk über den Finder

1. Wählen Sie im Finder die PGP-Laufwerksdatei (`.pgd`) für das Laufwerk aus, das Sie aktivieren möchten. Klicken Sie bei gedrückter Ctrl-Taste auf die ausgewählte PGD-Datei oder klicken Sie bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste darauf. Klicken Sie im Menü **PGP** auf **Aktivieren**. Das Dialogfeld „PGP-Passphrase eingeben“ wird angezeigt.
2. Geben Sie die Passphrase für das PGP Virtual Disk-Laufwerk ein, das Sie aktivieren möchten.

   Als zusätzliche Sicherheitsmaßnahme werden die für die Passphrase eingegebenen Zeichen in der Regel nicht auf dem Bildschirm angezeigt. Falls Sie jedoch sicher sind, dass Ihnen niemand zusieht (weder physisch noch über das Netzwerk), und wenn Sie die Zeichen der Passphrase beim Eingeben sehen möchten, klicken Sie auf **Eingabe ausgeblendet**.
3. Klicken Sie auf **OK**. Das PGP Virtual Disk-Laufwerk wird aktiviert.

So deaktivieren Sie ein PGP Virtual Disk-Laufwerk über den Finder

1. Wählen Sie die *aktivierte* PGP-Laufwerksdatei (`.pgd`) für das Laufwerk aus, das Sie deaktivieren möchten.
2. Klicken Sie bei gedrückter Ctrl-Taste auf die ausgewählte PGD-Datei oder klicken Sie bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste darauf. Wählen Sie aus dem Kontextmenü unter **PGP** **die Option** **Deaktivieren** aus. Das ausgewählte PGP Virtual Disk-Laufwerk wird deaktiviert.

Tipp: Wenn im Menü die Option **Aktivieren** angezeigt wird, ist das Laufwerk bereits deaktiviert.

PGP-Schlüssel importieren

PGP-Schlüssel können aus PGP Desktop als ASC-Dateien exportiert werden. Diese Methode bietet sich an, um Schlüssel zu sichern oder öffentliche Schlüssel mit anderen Personen auszutauschen. Wenn auf dem System eine ASC-Datei mit einem PGP-Schlüssel vorhanden ist, den Sie dem Schlüsselbund hinzufügen möchten, können Sie die Datei über den Finder importieren.

So importieren Sie Schlüssel aus einer ASC-Datei im Finder

1. Wählen Sie im Finder die PGP-Schlüsseldatei (ASC) aus, die die zu importierenden PGP-Schlüssel enthält.
2. Doppelklicken Sie auf die ausgewählte ASC-Datei. PGP Desktop wird geöffnet und das Dialogfeld „Schlüssel auswählen“ wird angezeigt.

3 Wählen Sie die PGP-Schlüssel aus, die Sie importieren möchten, und klicken Sie auf **OK**. Die ausgewählten Schlüssel werden dem Schlüsselbund hinzugefügt.

Tipp: Sie können einen Schlüssel auch importieren, indem Sie „Datei“ > „Öffnen“ auswählen und die gewünschte ASC-Datei suchen.

Öffentliche PGP-Schlüssel zum Schlüsselbund hinzufügen

Ihre PGP-Schlüssel werden von PGP Desktop an Schlüsselbunden gespeichert. Sie verfügen stets über einen privaten Schlüsselbund (`.skr`) mit privaten Schlüsseln und einen öffentlichen Schlüsselbund (`.pkr`) mit öffentlichen Schlüsseln.

Wenn auf dem System eine öffentliche Schlüsselbunddatei (nicht die aktive öffentliche Schlüsselbunddatei) vorhanden ist und Sie diese Datei dem Schlüsselbund hinzufügen möchten, können Sie hierfür den Finder verwenden.

So fügen Sie öffentliche PGP-Schlüssel aus einer Schlüsselbunddatei im Finder hinzu

1 Ziehen Sie im Finder den öffentlichen PGP-Schlüsselbund (`.pkr`) oder den privaten PGP-Schlüsselbund (`.skr`) in den aktiven Schlüsselbund im PGP Desktop-Fenster. Das Dialogfeld „Schlüssel auswählen“ wird geöffnet und die öffentlichen Schlüssel aus der ausgewählten öffentlichen Schlüsselbunddatei werden angezeigt.

2 Wählen Sie die Schlüssel aus, die Sie dem aktiven Schlüsselbund hinzufügen möchten, und klicken Sie auf **OK**. Für die Auswahl der gewünschten Schlüssel können Sie die Optionen **Alle auswählen**, **Keine auswählen** sowie die Umschalt- und die Befehlstaste verwenden. Das Dialogfeld „Schlüssel auswählen“ wird geschlossen und die ausgewählten Schlüssel werden dem aktiven Schlüsselbund hinzugefügt.

Tipp: Doppelklicken Sie im Finder auf den öffentlichen PGP-Schlüsselbund (`.pkr`) oder den privaten PGP-Schlüsselbund (`.skr`). Der neue Schlüsselbund wird in PGP Desktop unterhalb der bereits vorhandenen Schlüsselbunde als öffentlicher PGP-Schlüsselbund angezeigt.

Inhalt von PGP Zip-Archiven extrahieren

Wenn auf dem System ein PGP Zip-Archiv vorhanden ist, dessen Inhalt Sie extrahieren möchten, können Sie hierfür den Finder verwenden.

So extrahieren Sie den Inhalt eines PGP Zip-Archivs im Finder

1 Wählen Sie im Finder die PGP Zip-Archivdatei (.pgp) aus, deren Inhalt Sie extrahieren möchten.

2 Klicken Sie bei gedrückter Ctrl-Taste auf die ausgewählte PGP-Datei oder klicken Sie bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste darauf. Wählen Sie aus dem Kontextmenü im Menü PGP **die Option Entschlüsseln und verifizieren** aus. Das Dialogfeld „PGP-Passphrase eingeben“ wird angezeigt.

3 Geben Sie die Passphrase für das PGP Zip-Archiv ein, aus dem Sie Dateien extrahieren möchten, und klicken Sie auf **OK**. Die Dateien im Archiv werden im Finder an dem Speicherort extrahiert, an dem sich auch das Archiv befindet.

4 Wenn das Archiv signiert war, wird das Dialogfeld „Verifizierungsinformationen“ angezeigt.

PGP-Protokoll anzeigen

Das PGP-Protokoll gibt Aufschluss darüber, welche Aktionen von PGP Desktop ausgeführt werden, um Ihre Daten zu schützen. Weitere Informationen finden Sie unter *PGP-Protokoll anzeigen* (auf Seite 136).

6 Mit PGP Keys arbeiten

PGP Keys ist eine Funktion von PGP Desktop, mit der Sie eigene PGP-Schlüsselpaare und öffentliche Schlüssel anderer PGP Desktop-Benutzer erstellen und verwalten können.

In diesem Abschnitt wird beschrieben, wie Sie Schlüssel anzeigen, ein Schlüsselpaar erstellen, Ihren öffentlichen Schlüssel verteilen, die öffentlichen Schlüssel anderer Personen abrufen und mit Keyservern arbeiten.

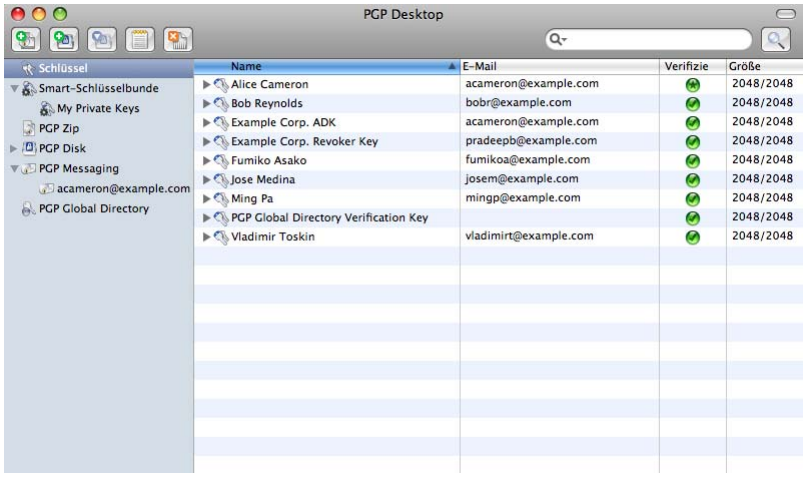
Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat der PGP Universal Server-Administrator möglicherweise bestimmte Funktionen deaktiviert. Wenn eine Funktion deaktiviert wurde, wird das entsprechende Bedienelement auf der linken Seite nicht angezeigt und das Menü und andere Optionen für diese Funktion sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn der PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Schlüssel anzeigen 48
Schlüsselpaare erstellen 50
Privaten Schlüssel schützen 54
Öffentliche Schlüssel verteilen 56
Öffentliche Schlüssel anderer Personen erhalten 60
Mit Keyservern arbeiten 62
Hauptschlüssel verwenden 63

Schlüssel anzeigen

Wenn Sie alle Schlüssel am lokalen Schlüsselbund anzeigen möchten, öffnen Sie PGP Desktop und klicken Sie auf **Schlüssel**.



Sie können auch die Funktion *Smart-Schlüsselbunde* verwenden. Ein Smart-Schlüsselbund besteht aus einem Satz von Schlüsseln, die bestimmten, von Ihnen festgelegten Kriterien entsprechen. Wenn Sie beispielsweise häufig Nachrichten an PGP Desktop-Benutzer in einer bestimmten E-Mail-Domäne senden, können Sie einen Smart-Schlüsselbund erstellen, der ausschließlich die Benutzer in dieser Domäne anzeigt. Der standardmäßige Smart-Schlüsselbund ist *Eigene private Schlüssel*.

Einige der häufiger verwendeten Aufgaben stehen im Arbeitsbereich von PGP Keys zur Verfügung. Hierbei handelt es sich um Folgende:

- Eine E-Mail-Nachricht an den Besitzer eines öffentlichen Schlüssels senden. Klicken Sie hierzu bei gedrückter Ctrl-Taste (oder mit der rechten Maustaste) in einer beliebigen Ansicht von PGP Keys auf einen öffentlichen Schlüssel auf den Schlüsselbunden und wählen Sie **E-Mail-Nachricht senden** aus.
- Wenn Sie eine Suche durchführen und einen öffentlichen Schlüssel auswählen, der bei der Suche gefunden wurde und sich nicht auf den lokalen Schlüsselbunden befindet, fügen Sie den Schlüssel dem Schlüsselbund hinzu. Klicken Sie hierzu bei gedrückter Ctrl-Taste (oder mit der rechten Maustaste) auf den Schlüssel und wählen Sie **Zu Standardschlüsselbund hinzufügen** aus.
- Zeigen Sie die Eigenschaften eines im Arbeitsbereich angezeigten Schlüssels an, indem Sie auf einen beliebigen Teil des aufgeführten Schlüssels doppelklicken, um das Dialogfeld „Schlüssel-Info“ für diesen Schlüssel zu öffnen.

Smart-Schlüsselbunde erstellen

So erstellen Sie einen Smart-Schlüsselbund

1. Öffnen Sie PGP Desktop.
2. Klicken Sie auf das Symbol **Schlüssel**.
3. Wählen Sie **Datei > Neu > Smart-Schlüsselbund** aus. Das Dialogfeld „Neuer Smart-Schlüsselbund“ wird angezeigt.
4. Geben Sie im Feld **Name des Smart-Schlüsselbunds** einen beschreibenden Namen für den neuen Smart-Schlüsselbund ein.
5. Wählen Sie im Menü **Schlüssel einschließen, die x der folgenden Bedingungen erfüllen** eine der folgenden Optionen aus:
   - **Beliebige**: Zeigt Schlüssel an, die beliebigen der angegebenen Kriterien entsprechen („OR“).
   - **Alle**: Zeigt nur Schlüssel an, die allen angegebenen Kriterien entsprechen („AND“).
6. Wählen Sie in der ersten Spalte für Übereinstimmungen eine der folgenden Optionen aus:
   - **Schlüssel ist**: Zeigt Schlüssel an, die die Kriterien erfüllen.
   - **Schlüssel ist nicht**: Zeigt Schlüssel an, die die Kriterien nicht erfüllen.
   - **Name**: Zeigt Schlüssel an, deren Name die angegebenen Kriterien erfüllt.
   - **E-Mail**: Zeigt Schlüssel an, deren E-Mail-Adresse die angegebenen Kriterien erfüllt.
   - **Schlüssel-ID**: Zeigt Schlüssel an, deren Schlüssel-ID die angegebenen Kriterien erfüllt.
   - **Schlüsselgröße**: Zeigt Schlüssel an, die der angegebenen Größe entsprechen.
   - **Erstellungsdatum**: Zeigt Schlüssel an, die am angegebenen Datum erstellt wurden.
   - **Ablaufdatum**: Zeigt Schlüssel an, die am angegebenen Datum ablaufen.
7. Die Optionen in der zweiten Spalte für Übereinstimmungen hängen von Ihrer Auswahl in der ersten Spalte ab. Folgende Optionen sind verfügbar:
   - **Öffentlich**: Zeigt nur öffentliche Schlüssel an.
   - **Privat**: Zeigt nur private Schlüssel an.
   - **Widerrufen**: Zeigt nur widerrufene Schlüssel an.
   - **Aktiviert**: Zeigt nur aktivierte Schlüssel an.

- **Abgelaufen**: Zeigt nur abgelaufene Schlüssel an.
- **Signiert von**: Zeigt nur Schlüssel an, die von der angegebenen Person signiert wurden.
- **Enthält**: Zeigt nur Schlüssel mit den angegebenen Kriterien an.
- **Enthält nicht**: Zeigt nur Schlüssel ohne die angegebenen Kriterien an.
- **Ist**: Zeigt Schlüssel an, die den angegebenen Kriterien (Name oder Datum) entsprechen.
- **Ist nicht**: Zeigt Schlüssel an, wenn die angegebenen Kriterien nicht erfüllt sind.
- **Ist mindestens**: Zeigt Schlüssel an, die mindestens der angegebenen Schlüsselgröße entsprechen.
- **Ist höchstens**: Zeigt Schlüssel an, die die angegebene Schlüsselgröße nicht überschreiten.
- **Ist am oder vor dem**: Zeigt Schlüssel an, wenn das angegebene Datum vor dem Datum in der Liste liegt oder diesem Datum entspricht.
- **Ist am oder nach dem**: Zeigt Schlüssel an, wenn das angegebene Datum nach dem Datum in der Liste liegt oder diesem Datum entspricht.

8. Das Textfeld, das für einige Elemente angezeigt wird, dient zur Eingabe von Text (beispielsweise E-Mail-Adressen oder Domänen; Platzhalterzeichen sind zulässig), Zahlen oder Datumsangaben.
9. Klicken Sie auf das Plussymbol, um weitere Zeilen für ein- oder auszuschließende Schlüssel hinzufügen. Klicken Sie auf das Minussymbol, um Zeilen zu entfernen.
10. Klicken Sie auf **Speichern**. Der Smart-Schlüsselbund wird in der Liste der Objekte angezeigt.

Wenn Sie diesen Smart-Schlüsselbund auswählen, werden nur die Schlüssel aufgeführt, die diesen Kriterien entsprechen. Der folgende Smart-Schlüsselbund entspricht beispielsweise den öffentlichen Schlüsseln der PGP Desktop-Benutzer in der Anwaltskanzlei Ihres Unternehmens.

Schlüsselpaare erstellen

Sie haben wahrscheinlich bereits ein PGP-Schlüsselpaar für den persönlichen Gebrauch erstellt, entweder mit dem Einrichtungsassistenten von PGP Desktop oder mit einer früheren Version von PGP Desktop. Ist dies nicht der Fall, müssen Sie es jetzt nachholen. Für fast alle Aktionen in PGP Desktop ist ein Schlüsselpaar erforderlich.

Achtung: Es ist nicht empfehlenswert, für sich selbst immer neue Schlüssel zu erstellen. Ein PGP-Schlüsselpaar ist wie ein digitaler Personalausweis oder Pass. Wenn Sie zu viele davon erstellen, verwirren Sie am Ende nicht nur sich selbst, sondern auch die Personen, die Ihnen verschlüsselte Nachrichten senden möchten. Es ist am besten, wenn Sie nur über einen einzigen Schlüssel verfügen, der alle von Ihnen verwendeten E-Mail-Adressen enthält. Das PGP Global Directory veröffentlicht jeweils nur ein Schlüsselpaar pro E-Mail-Adresse.

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist die Funktion zum Erstellen von Schlüsselpaaren möglicherweise deaktiviert.

So erstellen Sie ein PGP-Schlüsselpaar

1. Öffnen Sie PGP Desktop.
2. Wählen Sie im Menü **Datei** die Option **Neu > PGP-Schlüssel** aus. Das Dialogfeld zum Erstellen eines Schlüssels für sichere Kommunikation wird angezeigt. Den Informationen in diesem Dialogfeld können Sie entnehmen, was ein Schlüsselpaar ist und wie es verwendet wird.
3. Wenn Sie erweiterte Eigenschaften für den neuen Schlüssel angeben möchten, aktivieren Sie das Kontrollkästchen **Expertenmodus**. Weitere Informationen zu diesen Einstellungen finden Sie unter *Schlüsseleinstellungen im Expertenmodus* (auf Seite 52). Überspringen Sie diesen Schritt, wenn Sie den Expertenmodus nicht verwenden möchten.
4. Klicken Sie auf **Fortfahren**. Das Dialogfeld „Kontaktinformationen des Schlüssels einrichten“ wird angezeigt.
5. Geben Sie im Feld **Vollständiger Name** Ihren tatsächlichen Namen und im Feld **E-Mail-Adresse** **Ihre richtige E-Mail-Adresse ein.**

   Hinweis: Es ist nicht zwingend erforderlich, Ihren tatsächlichen Namen oder Ihre E-Mail-Adresse einzugeben. Durch die Verwendung Ihres echten Namens können andere Benutzer Sie jedoch einfacher als den Besitzer Ihres öffentlichen Schlüssels identifizieren. Ihre echte E-Mail-Adresse ist ebenfalls erforderlich, wenn Sie Ihren öffentlichen Schlüssel in das PGP Global Directory hochladen (das ihn auf einfache Weise für andere PGP Desktop-Benutzer verfügbar macht).
6. Klicken Sie auf **Fortfahren**. Das Dialogfeld „Passphrase des Schlüssels einrichten“ wird angezeigt.
7. Geben Sie eine Passphrase für den neuen Schlüssel ein und wiederholen Sie die Eingabe zur Bestätigung.

   Als zusätzliche Sicherheitsmaßnahme werden die für die Passphrase eingegebenen Zeichen in der Regel nicht auf dem Bildschirm angezeigt. Wenn Sie jedoch sicher sind, dass Sie nicht beobachtet werden, und die Zeichen beim Eingeben der Passphrase sehen möchten, klicken Sie auf **Tastatureingabe anzeigen**.

Achtung: Wählen Sie eine Passphrase, die Sie sich leicht merken können, ohne sie aufzuschreiben. Niemand, auch nicht die PGP Corporation, kann einen Schlüssel wiederherstellen, dessen Passphrase vergessen wurde, es sei denn, der PGP-Administrator hat eine PGP-Schlüssel-Wiederherstellungsrichtlinie für Ihr Unternehmen implementiert.

Die Passphrasen-Qualitätsanzeige kann als allgemeiner Anhaltspunkt für die Stärke der erstellten Passphrase verwendet werden. Dabei wird der Entropiewert der eingegebenen Passphrase mit einer echten zufälligen Zeichenkette mit 128 Bit verglichen. Dies entspricht dem Entropiewert eines AES-128-Schlüssels. Weitere Informationen finden Sie unter *Die Passphrasen-Qualitätsanzeige* (auf Seite 234).

8 Wenn die Passphrase im Mac OS X-Schlüsselbund gespeichert werden soll, aktivieren Sie das Kontrollkästchen.

9 Klicken Sie auf **Fortfahren**. Das Dialogfeld „Übersicht über die PGP-Schlüsselerstellung“ wird angezeigt.

10 Führen Sie bei Bedarf folgende Schritte aus:

- Wenn Sie Details zum Schlüssel anzeigen möchten, wählen Sie **Details anzeigen** aus.
- Wenn Sie Änderungen am Schlüssel vornehmen möchten, klicken Sie auf **Zurück**.

11 Klicken Sie auf **Schlüssel erstellen**. PGP Desktop erstellt das neue Schlüsselpaar. Dieser Vorgang kann einige Minuten dauern.

12 Wenn angezeigt wird, dass die Schlüsselerstellung abgeschlossen ist, klicken Sie auf **Beenden**.

Schlüsseleinstellungen im Expertenmodus

1 Wenn Sie im Dialogfeld „Neuer PGP-Schlüssel“ die Option **Expertenmodus** auswählen, müssen Sie zusätzlich zu Ihrem Namen und Ihrer E-Mail-Adresse auch Folgendes angeben:

- **Schlüsseltyp**: Wählen Sie zwischen **Diffie-Hellman/DSS** und **RSA**.

Hinweis: Ab PGP Desktop 9.0 wird das ältere RSA-Legacy-Schlüsselformat aus den frühen 90er Jahren nicht mehr in vollem Umfang unterstützt. Sie können keine **neuen** PGP-Schlüsselpaare mit dem RSA-Legacy-Schlüsselformat mehr erstellen. **Vorhandene** Schlüsselpaare in diesem Format werden jedoch weiterhin in PGP Desktop unterstützt.

- **Keyserver**: Geben Sie einen vertrauenswürdigen Keyserver an oder wählen Sie die Option **<Keiner>** aus.

- **Zulässige Komprimierung**: Deaktivieren Sie die Kontrollkästchen für alle Komprimierungstypen, die vom erstellten Schlüssel nicht unterstützt werden soll.
- **Zulässige Algorithmen**: Deaktivieren Sie die Kontrollkästchen für alle Algorithmen, die vom erstellten Schlüssel nicht unterstützt werden sollen.
- **Zulässige Hashes**: Deaktivieren Sie die Kontrollkästchen für alle Hashes, die vom erstellten Schlüsselpaar nicht unterstützt werden sollen.
- **Bevorzugter Algorithmus**: Wählen Sie den Algorithmus aus, der verwendet werden soll, wenn kein Algorithmus festgelegt wurde. Nur ein zulässiger Algorithmus kann als bevorzugter Algorithmus festgelegt werden.
- **Bevorzugter Hash**: Wählen Sie den Hash aus, der verwendet werden soll, wenn kein Hash festgelegt wurde. Nur ein zulässiger Hash kann als bevorzugter Hash festgelegt werden.
- **Schlüsselgröße**: Geben Sie zwischen 1024 Bit und 4096 Bit ein. Je größer der Schlüssel, desto sicherer ist er, aber seine Erstellung dauert auch entsprechend länger.
- **Schlüssel läuft ab**: Wählen Sie **Nie** aus oder geben Sie ein Ablaufdatum für den erstellten Schlüssel an.

2. Klicken Sie auf **Fortfahren**. Das Dialogfeld „Passphrase des Schlüssels einrichten“ wird angezeigt.
3. Geben Sie die Passphrase ein, die Sie für diesen Schlüssel verwenden möchten, und geben Sie sie im Feld **Passphrase bestätigen erneut ein. Es ist äußerst wichtig, dass Sie diese Passphrase geheim halten.**
4. Klicken Sie auf **Fortfahren.**
5. Überprüfen Sie die Informationen in der Übersicht und klicken Sie auf **Schlüssel erstellen**, um mit der Schlüsselerstellung zu beginnen. Das neue Schlüsselpaar wird von PGP Desktop erstellt.

   Dieser Vorgang kann einige Minuten dauern.
6. Wenn angezeigt wird, dass die Schlüsselerstellung abgeschlossen ist, klicken Sie auf **Weiter**. Sie werden aufgefordert, den öffentlichen Teil des soeben erstellten Schlüssels dem PGP Global Directory hinzuzufügen.
7. Lesen Sie den Text auf dem Bildschirm und klicken Sie auf **Weiter**.
8. Klicken Sie auf **Überspringen**, um zu verhindern, dass der öffentliche Schlüssel im PGP Global Directory veröffentlicht wird. Der Bildschirm „PGP Global Directory-Assistent wird abgeschlossen“ wird angezeigt.
9. Klicken Sie auf **Beenden**. Das neue PGP-Schlüsselpaar wurde erstellt. Es sollte im Arbeitsbereich von PGP Keys angezeigt werden. Falls es nicht aufgeführt ist, stellen Sie sicher, dass im Bedienfeld von PGP Keys entweder **Alle Schlüssel** oder **Eigene private Schlüssel** ausgewählt ist.

Privaten Schlüssel schützen

Die PGP Corporation empfiehlt, dass Sie die folgenden Schritte sofort nach dem Erstellen Ihres Schlüsselpaars ausführen:

Achtung: Wenn Sie diese Schritte nicht ausführen, kann dies in der Zukunft zu einem umfassenden Datenverlust führen.

- Erstellen Sie für den Fall, dass die ursprüngliche Datei des privaten Schlüssels beschädigt wird oder verloren geht, eine Sicherungskopie der Datei an einem anderen, sicheren Speicherplatz. Siehe *Sicherungskopien von privaten Schlüsseln erstellen* (auf Seite 55).
- Denken Sie über die gewählte Passphrase nach, um sicherzustellen, dass Sie sie nicht vergessen. Wenn Sie befürchten, dass Sie während der Erstellung des Schlüssels eine Passphrase festgelegt haben, die Sie möglicherweise wieder vergessen, ändern Sie sie JETZT in eine Passphrase, die Sie nicht vergessen. Informationen zum Ändern der Passphrase finden Sie unter *Passphrase ändern* (auf Seite 70, auf Seite 70).

Die Datei mit Ihrem privaten Schlüssel ist sehr wichtig, da nach dem Verschlüsseln der Daten an Ihren öffentlichen Schlüssel nur der entsprechende private Schlüssel zum Entschlüsseln der Daten verwendet werden kann. Dies trifft in gleicher Weise auf Ihre Passphrasen zu, denn der Verlust Ihres privaten Schlüssels oder der Passphrase bedeutet, dass Sie Daten, die an einen öffentlichen Schlüssel verschlüsselt wurden, nicht mehr entschlüsseln können. Wenn Sie Daten verschlüsseln, wird hierzu sowohl die Passphrase als auch der private Schlüssel verwendet. Sie benötigen beide, um die verschlüsselten Daten zu entschlüsseln. Nach der Verschlüsselung der Daten kann niemand – nicht einmal die PGP Corporation – die Daten ohne Ihre private Schlüsseldatei und Ihre Passphrase entschlüsseln.

Stellen Sie sich vor, Sie besitzen wichtige verschlüsselte Daten und vergessen dann die Passphrase oder verlieren den privaten Schlüssel. Auf die verschlüsselten Daten kann dann nicht mehr zugegriffen werden, sie können nicht mehr verwendet und auch nicht mehr wiederhergestellt werden.

Schlüssel und Schlüsselbunde schützen

Sie sollten nicht nur Sicherungskopien Ihrer Schlüssel erstellen, sondern auch besonders sorgsam darauf achten, wo Sie den privaten Schlüssel aufbewahren. Obwohl der private Schlüssel durch eine Passphrase geschützt ist, die nur Sie kennen sollten, ist es möglich, dass eine andere Person Ihre Passphrase in Erfahrung bringt und Ihren privaten Schlüssel zum Entschlüsseln von E-Mail-Nachrichten oder zum Fälschen Ihrer digitalen Signatur verwendet. Jemand könnte Ihnen beispielsweise über die Schulter blicken und beobachten, welche Tastatureingaben Sie vornehmen, oder die Tastatureingaben über das Netzwerk oder sogar über das Internet abfangen.

Damit andere Personen, die Ihre Passphrase abgefangen haben, Ihren privaten Schlüssel nicht nutzen können, sollten Sie diesen ausschließlich auf Ihrem eigenen Computer speichern. Falls der Computer mit einem Netzwerk verbunden ist, stellen Sie sicher, dass Ihre Dateien nicht automatisch in eine systemweite Sicherung einbezogen werden, über die andere Personen Zugriff auf Ihren privaten Schlüssel erhalten könnten. Da ein Zugriff auf Computer in einem Netzwerk recht problemlos möglich ist, sollten Sie Ihren privaten Schlüssel auf einer Diskette speichern, falls Sie mit extrem vertraulichen Daten arbeiten. Diese Diskette kann wie ein traditioneller Schlüssel immer dann eingesteckt werden, wenn Sie private Informationen lesen oder signieren möchten.

Als weitere Sicherheitsmaßnahme könnten Sie Ihrer privaten Schlüsselbunddatei einen anderen Namen zuweisen und sie nicht am Standardspeicherort speichern. Geben Sie im Dialogfeld „Optionen“ auf der Registerkarte „Schlüssel“ einen Namen und einen Speicherort für Ihre privaten und öffentlichen Schlüsselbunddateien an.

Ihre privaten und öffentlichen Schlüssel werden in getrennten Schlüsselbunddateien gespeichert. Sie können sie an einen anderen Speicherplatz auf der Festplatte oder auf einer Diskette kopieren. Standardmäßig werden der private Schlüsselbund (`secring.skr`) und der öffentliche Schlüsselbund (`pubring.pkr`) zusammen mit anderen Programmdateien im PGP-Ordner gespeichert. Sicherungskopien können an einem beliebigen Speicherort gespeichert werden.

Für Schlüssel, die auf einer Smartcard erstellt wurden, können keine Sicherungskopien erstellt werden, da der private Teil Ihres Schlüsselpaars nicht exportierbar ist. (Schlüssel können nur unter Windows auf einer Smartcard erstellt werden.)

Sie können PGP Desktop so konfigurieren, dass Schlüsselbunde automatisch nach dem Beenden von >prod< gesichert werden. Legen Sie die Sicherungsoptionen für Schlüsselbunde im Dialogfeld „Optionen“ auf der Registerkarte „Schlüssel“ (Windows) bzw. im Dialogfeld „Einstellungen“ im Bereich „Schlüssel“ (Mac OS X) fest.

Sicherungskopien von privaten Schlüsseln erstellen

So erstellen Sie eine Sicherungskopie Ihres privaten Schlüssels

1. Klicken Sie unter „Smart-Schlüsselbunde“ auf **Eigene private Schlüssel**.
2. Wählen Sie das Symbol für Ihr Schlüsselpaar aus.
3. Klicken Sie im Menü **Datei** auf **Exportieren**.
4. Geben Sie im Feld **Speichern unter** einen Namen für die Datei ein und geben Sie den Speicherort im Feld **Wo** an.
5. Aktivieren Sie das Kontrollkästchen **Private Schlüssel einschließen**. Dies ist wichtig, da andernfalls nur der *öffentliche* Schlüssel exportiert wird.

6 Klicken Sie auf **Speichern**.

7 Kopieren Sie die Datei an einen sicheren Speicherort. Hierbei kann es sich um eine CD handeln, die sorgfältig archiviert wird, um einen anderen PC oder um ein USB-Flash-Laufwerk, das an einem sicheren Ort aufbewahrt wird. Denken Sie daran, dass diese Datei nicht an andere Personen weitergegeben werden darf, da sie sowohl Ihren privaten als auch Ihren öffentlichen Schlüssel enthält.

Hinweis: Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten und den SKM-Schlüsselmodus verwenden, können Sie Ihren Schlüssel nicht mit dieser Methode exportieren. Exportieren Sie Ihr Schlüsselpaar, indem Sie den PGP Universal Server-Administrator bitten, das Schlüsselpaar über die Verwaltungskonsole zu exportieren. Informationen zum Ermitteln des Schlüsselmodus finden Sie unter *Schlüsselmodi* (auf Seite 132).

Vorgehensweise bei verlorenen Schlüsseln

Wenn Sie Ihren Schlüssel verlieren und nicht über eine Sicherungskopie verfügen, von der Sie den Schlüssel wiederherstellen können, können Sie die Informationen, die mit dem Schlüssel verschlüsselt wurden, nie mehr entschlüsseln. Sie können den Schlüssel jedoch wiederherstellen, wenn der PGP-Administrator eine Richtlinie zur Schlüsselwiederherstellung für Ihr Unternehmen implementiert hat. Weitere Informationen finden Sie unter *PGP-Schlüsselwiederherstellung* (siehe "*Schlüssel mit PGP Universal Server wiederherstellen*" auf Seite 90, "*Vorgehensweise bei verloren gegangenen Schlüsseln oder Passphrasen*" auf Seite 89). Sie können sich auch an den PGP-Administrator wenden.

Öffentliche Schlüssel verteilen

Nachdem Sie ein PGP Desktop-Schlüsselpaar erstellt haben, müssen Sie den öffentlichen Schlüssel an die Personen übermitteln, mit denen Sie verschlüsselte Nachrichten austauschen möchten.

Sie stellen den öffentlichen Schlüssel anderen Personen bereit, damit diese Ihnen verschlüsselte Informationen senden und Ihre digitale Signatur verifizieren können. Sie benötigen den öffentlichen Schlüssel dieser Personen, um ihnen verschlüsselte Nachrichten senden zu können.

Es gibt verschiedene Möglichkeiten, den öffentlichen Schlüssel zu verteilen:

- *Veröffentlichen Sie den Schlüssel im PGP Global Directory* (siehe "*Öffentliche Schlüssel auf einem Keyserver ablegen*" auf Seite 57).

  Im Allgemeinen ist keine der anderen Verfahren mehr erforderlich, wenn der Schlüssel in diesem Verzeichnis veröffentlicht wurde.

- *Fügen Sie den öffentlichen Schlüssel in eine E-Mail-Nachricht ein* (siehe "*Öffentliche Schlüssel in E-Mail-Nachrichten einfügen*" auf Seite 58).
- *Exportieren Sie den öffentlichen Schlüssel oder kopieren Sie ihn in eine Textdatei* (siehe "*Öffentliche Schlüssel in Dateien exportieren*" auf Seite 59).

Unter Windows ist auch Folgendes möglich:

- Kopieren Sie die Informationen von einer Smartcard direkt auf den Schlüsselbund einer anderen Person.

Öffentliche Schlüssel auf einem Keyserver ablegen

Die beste Methode zur Bereitstellung eines öffentlichen Schlüssels an andere besteht darin, ihn auf einem öffentlichen Keyserver (einer großen Datenbank mit Schlüsseln) abzulegen, damit alle darauf zugreifen können. Auf diese Weise können Ihnen andere Personen verschlüsselte E-Mail-Nachrichten senden, ohne ausdrücklich eine Kopie Ihres Schlüssels anfordern zu müssen. Gleichzeitig müssen weder Sie noch andere Personen eine große Anzahl öffentlicher Schlüssel speichern, die Sie selten verwenden.

Weltweit gibt es zahlreiche Keyserver (darunter das PGP Global Directory), auf denen Sie Ihren Schlüssel allgemein zugänglich machen können. Falls Sie PGP Desktop in einer Domäne einsetzen, die durch einen PGP Universal Server geschützt ist, hat der PGP-Administrator PGP Desktop mit entsprechenden Einstellungen vorkonfiguriert.

Wenn Sie einen öffentlichen Keyserver nutzen, beachten Sie beim Senden des Schlüssels Folgendes:

- Ist dies tatsächlich der Schlüssel, den Sie verwenden möchten? Andere Personen, die mit Ihnen kommunizieren möchten, könnten wichtige Informationen an diesen Schlüssel verschlüsseln. Aus diesem Grund sollten Sie nur Schlüssel auf einem Keyserver platzieren, die tatsächlich von anderen verwendet werden sollen.
- Können Sie sich an die Passphrase für diesen Schlüssel erinnern, damit Sie Daten abrufen können, die an den Schlüssel verschlüsselt wurden, oder damit Sie den Schlüssel widerrufen können, falls Sie ihn nicht mehr verwenden möchten?
- Anders als beim PGP Global Directory bleibt ein einmal hochgeladener Schlüssel auf dem Server. Einige öffentliche Keyserver lassen das Löschen von Schlüsseln nicht zu. Andere Server wiederum bieten Replizierungsfunktionen, die Schlüssel auch auf andere Keyserver kopieren. Selbst wenn Sie einen Schlüssel von einem Server löschen, könnte er später wieder auf einem anderen Server auftauchen.

Die meisten Benutzer legen den öffentlichen Schlüssel unmittelbar nach dem Erstellen des Schlüsselpaars im PGP Global Directory ab. Wenn Sie den Schlüssel bereits im PGP Global Directory abgelegt haben, müssen Sie diesen Vorgang nicht wiederholen. In den meisten Fällen ist es nicht notwendig, den Schlüssel auf einem anderen Keyserver zu veröffentlichen. Beachten Sie auch, dass Schlüssel auf anderen Keyservern u. U. nicht verifiziert werden, sodass möglicherweise ein höherer Zeitaufwand Ihrerseits erforderlich ist, um sich mit dem Besitzer des Keyservers in Kontakt zu setzen und den Fingerabdruck zu verifizieren.

So senden Sie Ihren öffentlichen Schlüssel manuell an einen Keyserver

1. Öffnen Sie PGP Desktop.
2. Halten Sie die Ctrl-Taste gedrückt und klicken Sie auf das Schlüsselpaar, dessen öffentlichen Schlüssel Sie an den Keyserver senden möchten.
3. Klicken Sie auf **Schlüssel an Server senden** und wählen Sie in der Liste den Keyserver aus, an den Sie den öffentlichen Schlüssel senden möchten. Falls der Keyserver, an den Sie den öffentlichen Schlüssel senden möchten, nicht in der Liste aufgeführt wird, finden Sie weitere Informationen unter *Mit Keyservern arbeiten* (auf Seite 62).

Sobald Sie eine Kopie Ihres öffentlichen Schlüssels auf einem Keyserver platziert haben, ist er für andere Personen verfügbar, die Ihnen verschlüsselte Daten senden oder Ihre digitale Signatur verifizieren möchten. Auch wenn Sie andere Benutzer nicht ausdrücklich auf Ihren öffentlichen Schlüssel hinweisen, können diese eine Kopie davon abrufen, indem sie den Keyserver nach Ihrem Namen oder Ihrer E-Mail-Adresse durchsuchen.

Viele Benutzer geben die Webadresse für ihren öffentlichen Schlüssel am Ende ihrer E-Mail-Nachrichten an. In den meisten Fällen kann der Empfänger einfach auf die Adresse doppelklicken, um auf eine Kopie Ihres Schlüssels auf dem Server zuzugreifen. Einige Benutzer drucken ihren PGP-Fingerabdruck sogar auf ihre Visitenkarte, um die Verifizierung zu erleichtern.

Öffentliche Schlüssel in E-Mail-Nachrichten einfügen

Eine weitere praktische Methode zur Übermittlung des öffentlichen Schlüssels an andere ist das Einfügen des Schlüssels in eine E-Mail-Nachricht.

Wenn Sie einer anderen Person Ihren öffentlichen Schlüssel senden, achten Sie darauf, die E-Mail-Nachricht zu signieren. Auf diese Weise kann der Empfänger Ihre Signatur verifizieren und sicherstellen, dass niemand die Daten bei der Übermittlung verfälscht hat. Falls Ihr Schlüssel jedoch noch nicht von einer Vertrauensperson signiert wurde, können die Empfänger Ihrer Signatur nur dann sicher sein, dass die Signatur von Ihnen stammt, wenn Sie den Fingerabdruck auf Ihrem Schlüssel verifizieren.

So hängen Sie Ihren öffentlichen Schlüssel an eine E-Mail-Nachricht an

1. Öffnen Sie PGP Desktop.
2. Öffnen Sie den E-Mail-Client, erstellen Sie eine neue Nachricht und fügen Sie den Empfänger hinzu, dem Sie den öffentlichen Schlüssel senden möchten.
3. Ziehen Sie das Schlüsselpaar aus PGP Desktop in die E-Mail-Nachricht und legen Sie es dort ab.
4. Senden Sie die Nachricht.

Wenn dieses Verfahren in Ihrem Fall nicht funktioniert, können Sie alternativ PGP Desktop öffnen, Ihr Schlüsselpaar auswählen und dann auf **Bearbeiten > Kopieren** klicken. Öffnen Sie eine E-Mail-Nachricht und fügen Sie den öffentlichen Schlüssel in den Nachrichtentext ein. Bei einigen E-Mail-Anwendungen können Sie den Schlüssel einfach aus PGP Desktop in den Text der E-Mail-Nachricht ziehen, um die Daten des öffentlichen Schlüssels zu übertragen.

Öffentliche Schlüssel in Dateien exportieren

Eine andere Methode zum Verteilen des öffentlichen Schlüssels besteht darin, ihn in eine Datei zu exportieren. Diese Datei stellen Sie dann der Person zur Verfügung, mit der Sie sicher kommunizieren möchten.

Es gibt drei Möglichkeiten, den öffentlichen Schlüssel in eine Datei zu exportieren oder ihn in einer Datei zu speichern:

- Wählen Sie das Schlüsselpaar aus und klicken Sie auf **Datei > Exportieren**. Geben Sie einen Namen und einen Speicherort für die Datei an und klicken Sie auf **Speichern**. Achten Sie darauf, den privaten Schlüssel *keinesfalls* zusammen mit dem öffentlichen Schlüssel zu speichern, wenn Sie diese Datei an andere Personen weitergeben möchten.
- Klicken Sie bei gedrückter Ctrl-Taste auf den Schlüssel, den Sie in einer Datei speichern möchten. Wählen Sie **Exportieren**, geben Sie einen Namen und einen Speicherort für die Datei ein und klicken Sie auf **Speichern**. Achten Sie darauf, den privaten Schlüssel *keinesfalls* zusammen mit dem öffentlichen Schlüssel zu speichern, wenn Sie diese Datei an andere Personen weitergeben möchten.
- Wählen Sie das Schlüsselpaar aus und klicken Sie auf **Bearbeiten > Kopieren**. Öffnen Sie ein Textbearbeitungsprogramm und wählen Sie **Einfügen** aus, um die Schlüsselinformationen in die Textdatei einzufügen. Speichern Sie dann die Datei. Sie können die Datei danach per E-Mail versenden oder an andere Personen weitergeben. Der Empfänger muss auf seinem System PGP Desktop verwenden, um den öffentlichen Teil des Schlüssels abrufen zu können.

Öffentliche Schlüssel anderer Personen erhalten

Ebenso, wie Sie Ihren öffentlichen Schlüssel an alle Personen weitergeben müssen, die Ihnen verschlüsselte E-Mail-Nachrichten senden oder Ihre digitale Signatur verifizieren möchten, benötigen Sie die öffentlichen Schlüssel anderer Personen, denen Sie verschlüsselte E-Mail-Nachrichten senden oder deren digitale Signatur Sie verifizieren möchten.

Es gibt verschiedene Möglichkeiten, den öffentlichen Schlüssel einer anderen Person zu erhalten:

- Automatisches Abrufen des verifizierten Schlüssels aus dem PGP Global Directory
- Manuelles Suchen des Schlüssels auf einem öffentlichen Keyserver
- Automatisches Hinzufügen des öffentlichen Schlüssels aus einer E-Mail-Nachricht an den eigenen Schlüsselbund
- Importieren des öffentlichen Schlüssels aus einer exportierten Datei
- Abrufen des Schlüssels vom PGP Universal Server Ihrer Organisation

Öffentliche Schlüssel sind lediglich Textblöcke. Sie können dem Schlüsselbund problemlos hinzugefügt werden, indem sie aus einer Datei importiert oder aus einer E-Mail-Nachricht kopiert und in den öffentlichen Schlüsselbund in PGP Desktop einfügt werden.

Öffentliche Schlüssel von einem Keyserver abrufen

Wenn der Empfänger der verschlüsselten E-Mail-Nachricht ein erfahrener PGP Desktop-Benutzer ist, befindet sich wahrscheinlich eine Kopie seines öffentlichen Schlüssels im PGP Global Directory oder auf einem anderen öffentlichen Keyserver. Somit können Sie jederzeit eine Kopie seines aktuellen Schlüssels abrufen, wenn Sie eine E-Mail-Nachricht an diesen Empfänger senden möchten, und müssen auf Ihrem öffentlichen Schlüsselbund keine unüberschaubare Zahl von Schlüsseln speichern.

Es gibt eine Vielzahl von öffentlichen Keyservern, z. B. das von der PGP Corporation gehostete PGP Global Directory, auf denen die Schlüssel der meisten PGP-Benutzer zu finden sind. Wenn Ihnen der Empfänger keine Internet-Adresse mitgeteilt hat, unter der sein öffentlicher Schlüssel gespeichert ist, können Sie auf einen beliebigen Keyserver zugreifen und nach dem Namen oder der E-Mail-Adresse des Benutzers suchen. Die Suche führt nicht in jedem Fall zum Erfolg, da nicht alle öffentlichen Keyserver regelmäßig mit dem Schlüsseldatenbestand der anderen Server synchronisiert werden.

Falls Sie in einer Domäne arbeiten, die durch einen PGP Universal Server geschützt ist, kann der PGP-Administrator ggf. vorgeben, dass der in den PGP Universal Server integrierte Keyserver verwendet werden muss. In diesem Fall ist PGP Desktop wahrscheinlich bereits für den Zugriff auf den entsprechenden PGP Universal Server konfiguriert.

Der PGP Universal Server ist seinerseits standardmäßig für die Kommunikation mit dem PGP Global Directory konfiguriert. Dadurch werden Schlüsselsuche und -verifizierung auf verschiedene PGP-Anwendungen verteilt.

So rufen Sie den öffentlichen Schlüssel einer anderen Person von einem Keyserver ab

1. Öffnen Sie PGP Desktop.
2. Klicken Sie auf das Symbol des PGP Global Directory oder eines anderen Keyservers, den Sie durchsuchen möchten. Im Arbeitsbereich wird der Bildschirm „Nach Schlüsseln suchen“ angezeigt.
3. Legen Sie die Suchkriterien fest und klicken Sie auf **Suchen**.
   - Wenn der gewünschte Keyserver nicht angezeigt wird, wählen Sie im Menü **Schlüssel** die Option **Keyserver hinzufügen** aus und konfigurieren Sie den Keyserver.
   - Bei der Suche nach Schlüsseln auf einem Keyserver können Sie Angaben für verschiedene Schlüsselmerkmale festlegen. Zudem können Sie nach dem Ausschlussverfahren suchen, indem Sie beispielsweise das Suchkriterium „Benutzer-ID ist nicht Charles“ verwenden.

   Die Ergebnisse der Suche werden angezeigt.
4. Wenn bei der Suche ein öffentlicher Schlüssel gefunden wird, den Sie dem Schlüsselbund hinzufügen möchten, klicken Sie bei gedrückter Ctrl-Taste auf den Schlüssel und wählen Sie **Zu Standardschlüsselbund hinzufügen** aus. Der ausgewählte Schlüssel wird dem Schlüsselbund hinzugefügt.

Tipp: Wenn Sie mithilfe der Suchkriterien nach einem sehr gängigen Namen suchen (z. B. „Name enthält Stefan“), wird nur die erste Übereinstimmung zurückgegeben. Dieses Verhalten ist beabsichtigt, um das nicht autorisierte, massenhafte Abfragen von Schlüsseln (das so genannte Harvesting) zum Zweck des Phishing zu verhindern. Wenn Sie gängige Namen oder Domänen verwenden, müssen Sie möglicherweise den vollständigen Namen oder die gesamte E-Mail-Adresse eingeben, um den richtigen Schlüssel zu finden.

Öffentliche Schlüssel aus E-Mail-Nachrichten übernehmen

Eine praktische Methode zum Übermitteln eines öffentlichen Schlüssels besteht darin, den Schlüssel als Anlage einer E-Mail-Nachricht zu senden.

So fügen Sie einen öffentlichen Schlüssel hinzu, den Sie als Anlage einer E-Mail-Nachricht erhalten

1. Öffnen Sie die E-Mail-Nachricht.
2. Doppelklicken Sie auf die ASC-Datei, die den öffentlichen Schlüssel enthält. PGP Desktop erkennt das Dateiformat und öffnet das Dialogfeld „Schlüssel auswählen“.
3. Bestätigen Sie die Abfrage zum Öffnen der Datei.
4. Wählen Sie die öffentlichen Schlüssel aus, die Sie Ihrem Schlüsselbund hinzufügen möchten, und klicken Sie auf **Importieren**.

Mit Keyservern arbeiten

PGP Desktop erkennt folgende Arten von Keyservern:

- **PGP Universal-Keyserver**: Wenn Sie PGP Desktop in einer Domäne verwenden, die durch einen PGP Universal Server geschützt ist, ist PGP Desktop für die ausschließliche Kommunikation mit dem Keyserver vorkonfiguriert, der in den entsprechenden PGP Universal Server integriert ist. Für PGP Desktop handelt es sich hierbei um einen vertrauenswürdigen Keyserver. PGP Desktop vertraut daher automatisch allen Schlüsseln auf diesem Keyserver, sofern der PGP Universal Server nicht signalisiert, dass der betreffende Schlüssel nicht vertrauenswürdig ist. Dies kann beispielsweise bei der Verifizierung der Signaturen von Remoteschlüsseln der Fall sein.
- **PGP Global Directory**: Wenn Sie PGP Desktop außerhalb einer Domäne einsetzen, die durch einen PGP Universal Server geschützt ist, ist PGP Desktop für die Kommunikation mit dem PGP Global Directory vorkonfiguriert.

  Das PGP Global Directory ist ein kostenloser, frei zugänglicher Keyserver, der von der PGP Corporation gehostet wird. Zudem ermöglicht der Server den schnellen und einfachen Zugriff auf die PGP-Schlüssel. Das PGP Global Directory nutzt eine Keyserver-Technologie der nächsten Generation. Mit dieser Technologie werden die Schlüssel verifiziert, die einer E-Mail-Adresse zugeordnet sind, sodass der Keyserver nicht durch unbenutzte oder gefälschte Schlüssel, durch mehrere Schlüssel pro E-Mail-Adresse und andere Probleme belastet wird, die bei älteren Keyservern anzutreffen waren. Außerdem können Sie Ihre eigenen Schlüssel verwalten und u. a. Ihre eigenen Schlüssel ersetzen und löschen sowie Schlüsseln weitere E-Mail-Adressen hinzufügen. Durch die Verwendung des PGP Global Directory haben Sie wesentlich bessere Chancen, den öffentlichen Schlüssel einer Person zu finden, der Sie sichere Nachrichten senden möchten.

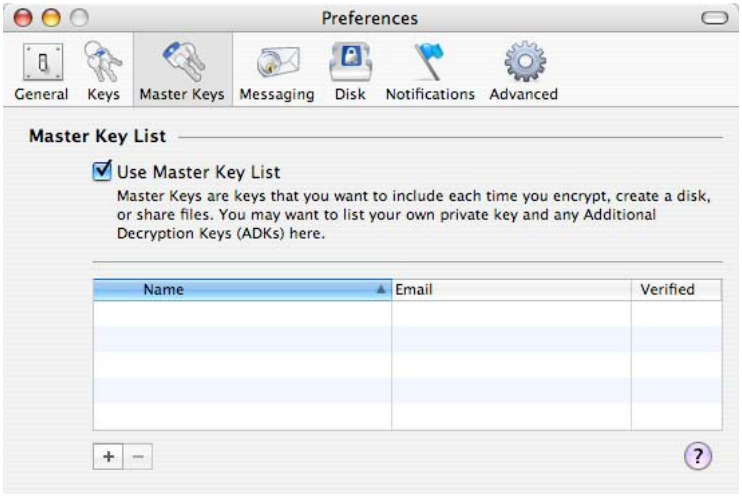
Das PGP Global Directory wird von PGP Desktop als vertrauenswürdiger Keyserver angesehen. PGP Desktop vertraut daher automatisch allen Schlüsseln, die dort gefunden werden. Während des anfänglichen Verbindungsaufbaus mit dem PGP Global Directory wird der PGP Global Directory-Überprüfungsschlüssel heruntergeladen, signiert und von dem Schlüssel als vertrauenswürdig eingestuft, den Sie im PGP Global Directory veröffentlichen. Somit werden alle vom PGP Global Directory verifizierten Schlüssel von Ihrer Installation von PGP Desktop als gültig betrachtet.

- **PGP Universal-Dienstprotokoll**: Das PGP Universal-Dienstprotokoll (USP) ist ein SOAP-Protokoll, das über HTTP/HTTPS-Standardports ausgeführt wird. Dies ist der Standardmechanismus für die Schlüsselsuche. Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten, wird PGP USP für alle Anforderungen für die Schlüsselsuche sowie für die gesamte Kommunikation zwischen dem PGP Universal Server und PGP Desktop verwendet.
- **Andere Keyserver**: In den meisten Fällen handelt es sich hierbei um andere öffentliche Keyserver. Unter Umständen können Sie jedoch z. B. über Ihr Unternehmen auf einen privaten Keyserver zugreifen.

Weitere Informationen zum Arbeiten mit Keyservern finden Sie unter *Schlüsseleinstellungen* (auf Seite 220).

Hauptschlüssel verwenden

Die Hauptschlüsselliste enthält eine Reihe von Schlüsseln, die Sie standardmäßig jedes Mal hinzufügen möchten, wenn Sie Schlüssel für Messaging, Laufwerksverschlüsselung oder PGP Zip auswählen. Die betreffenden Schlüssel müssen in diesem Fall nicht mehr in das Feld **Empfänger** gezogen werden.



Wenn Sie die Hauptschlüsselliste verwenden möchten, aktivieren Sie das Kontrollkästchen **Hauptschlüssellisteverwenden. Sie können nur Schlüssel in die Hauptschlüsselliste aufnehmen bzw. daraus entfernen, wenn dieses Kontrollkästchen aktiviert ist.**

Hinweis: Wenn Sie Ihren Schlüssel mithilfe des Einrichtungsassistenten erstellt haben, wird er der Hauptschlüsselliste automatisch hinzugefügt. Wenn Sie die Schlüsselerstellung übersprungen und den Schlüssel in PGP Desktop importiert haben, wird der Schlüssel nicht automatisch der Liste hinzugefügt.

Der Hauptschlüsselliste Schlüssel hinzufügen

▸ **So fügen Sie der Hauptschlüsselliste Schlüssel hinzu**

1. Öffnen Sie PGP Desktop.
2. Klicken Sie auf **PGP > Einstellungen**.
3. Klicken Sie auf das Symbol **Hauptschlüssel**.
4. Klicken Sie auf das Plussymbol unter der Schlüsselliste. Das Dialogfeld „Hauptschlüssel auswählen“ wird angezeigt.
5. Wählen Sie in der Liste **Name** auf der linken Seite die Schlüssel aus, die Sie verwenden möchten. Halten Sie beim Klicken die Umschalt- bzw. die Befehlstaste gedrückt, um mehrere Schlüssel auszuwählen.
6. Klicken Sie nach Auswahl der gewünschten Schlüssel auf **OK.** Die ausgewählten Schlüssel werden in der Hauptschlüsselliste angezeigt.

Schlüssel aus der Hauptschlüsselliste löschen

▸ **So entfernen Sie Schlüssel aus der Hauptschlüsselliste**

1. Öffnen Sie PGP Desktop.
2. Klicken Sie auf **PGP > Einstellungen**.
3. Klicken Sie auf das Symbol **Hauptschlüssel**.
4. Wählen Sie die Schlüssel aus, die Sie entfernen möchten. Halten Sie beim Klicken die Umschalt- bzw. die Befehlstaste gedrückt, um mehrere Schlüssel auszuwählen.
5. Klicken Sie auf das Minussymbol unter der Schlüsselliste. Die Schlüssel werden entfernt.

7 PGP-Schlüssel verwalten

In diesem Abschnitt wird beschrieben, wie Sie Schlüssel mit PGP Desktop verwalten.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat der PGP Universal Server-Administrator möglicherweise bestimmte Funktionen deaktiviert. Wenn eine Funktion deaktiviert wurde, wird das entsprechende Bedienelement auf der linken Seite nicht angezeigt und das Menü und andere Optionen für diese Funktion sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn der PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Schlüsseleigenschaften anzeigen und festlegen 66
Fotos hinzufügen und entfernen 66
Benutzernamen und E-Mail-Adressen in einem Schlüssel verwalten 68
Schlüssel und X.509-Zertifikate importieren 69
Passphrase ändern 70
Schlüssel, Benutzer-IDs und Signaturen löschen 71
Öffentliche Schlüssel deaktivieren und aktivieren 72
Einen öffentlichen Schlüssel verifizieren 72
Öffentliche Schlüssel signieren 74
Vertrauen für Schlüsselvalidierungen gewähren 76
Mit Unterschlüsseln arbeiten 77
Mit ADKs arbeiten 82
Mit Widerrufern arbeiten 84
Schlüssel teilen und wieder zusammenfügen 86
Vorgehensweise bei verloren gegangenen Schlüsseln oder Passphrasen 89
Schlüssel schützen 94

Schlüsseleigenschaften anzeigen und festlegen

Im Dialogfeld „Schlüssel-Info“ werden alle erforderlichen Informationen zu einem Schlüssel angezeigt. Im Arbeitsbereich von PGP Keys können die folgenden wichtigen Details zu Ihren Schlüsseln angezeigt werden:

- Name
- E-Mail-Adresse
- Gültigkeit
- Größe
- Schlüssel-ID
- Vertrauen
- Erstellungsdatum
- Ablaufdatum
- ADK
- Status
- Schlüsselbeschreibung
- Schlüsselverwendung

Hinweis: Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten und den SKM-Schlüsselmodus verwenden, können Sie keine Änderungen an Ihrem Schlüssel vornehmen. Zudem laufen SKM-Schlüssel grundsätzlich nicht ab. Informationen zum Ermitteln des Schlüsselmodus finden Sie unter *Schlüsselmodi* (auf Seite 132).

So zeigen Sie die Eigenschaften eines Schlüssels an

1. Öffnen Sie PGP Desktop und klicken Sie auf das Element „Schlüssel“. Alle Schlüssel am Schlüsselbund werden angezeigt.
2. Doppelklicken Sie auf den Schlüssel, dessen Eigenschaften Sie ermitteln möchten. Das Dialogfeld „Schlüsseleigenschaften“ wird für den ausgewählten Schlüssel angezeigt.

Fotos hinzufügen und entfernen

Sie können Diffie-Hellman/DSS- und RSA-Schlüsseln ein Foto hinzufügen.

Hinweis: Wenn Sie Schlüsselinformationen ändern oder hinzufügen, achten Sie darauf, den Schlüssel auf dem Keyserver zu aktualisieren, damit stets Ihr aktueller Schlüssel verfügbar ist.

Achtung: Obwohl Sie zur Verifizierung das einem Schlüssel beigefügte Foto anzeigen können, ist letztlich der digitale Fingerabdruck maßgeblich. Prüfen und vergleichen Sie diesen stets.

So fügen Sie dem Schlüssel ein Foto hinzu

1. Öffnen Sie PGP Desktop und klicken Sie auf **Eigene private Schlüssel**.
2. Doppelklicken Sie auf den privaten Schlüssel, dem Sie das Foto hinzufügen möchten. Das Dialogfeld „Schlüssel-Info“ des ausgewählten Schlüssels wird angezeigt.
3. Klicken Sie auf das Plussymbol unter dem aktuellen Foto für den Schlüssel. Das Dialogfeld „Foto hinzufügen“ wird angezeigt.
4. Ziehen Sie das gewünschte Foto in den leeren Bereich des Dialogfelds „Foto hinzufügen“ oder fügen Sie es ein.

   Hinweis: Das Foto kann aus der Zwischenablage kopiert werden und es kann sich um eine JPG- bzw. BMP-Datei handeln. Sie erzielen die beste Bildqualität, wenn Sie das Foto auf 120 x 144 Pixel zuschneiden, bevor Sie es hinzufügen. Andernfalls wird das Foto von PGP Desktop skaliert.
5. Klicken Sie auf **OK**. Sofern die Passphrase für den zu ändernden Schlüssel nicht zwischengespeichert ist, wird das Dialogfeld „PGP-Passphrase eingeben“ angezeigt.
6. Geben Sie die Passphrase für den Schlüssel ein, den Sie ändern, und klicken Sie auf **OK**. Die Foto-ID wird dem privaten Schlüssel hinzugefügt.

So zeigen Sie eine Vergrößerung des Fotos an

- Klicken Sie auf die Lupe unter dem Foto. Es wird ein Fenster mit einer größeren Version der Foto-ID angezeigt. Klicken Sie zum Entfernen der Vergrößerung in das Fenster.

So löschen Sie eine Foto-ID

1. Klicken Sie auf das Minussymbol unter dem Foto. Ein Bestätigungsdialogfeld wird angezeigt.
2. Bestätigen Sie den Vorgang. Das Foto wird vom Schlüssel entfernt.

So kopieren Sie eine Foto-ID

- Klicken Sie mit der rechten Maustaste im Dialogfeld „Schlüsseleigenschaften“ auf das Foto und wählen Sie **Foto-ID kopieren** aus. Dann können Sie das Foto in einen anderen Schlüssel oder in ein Grafikprogramm einfügen.

Benutzernamen und E-Mail-Adressen in einem Schlüssel verwalten

PGP Desktop unterstützt mehrere Benutzernamen und E-Mail-Adressen auf einem Schlüsselpaar. Anhand dieser Namen und E-Mail-Adressen können andere Personen Ihren Schlüssel ermitteln, um Ihnen verschlüsselte Nachrichten zu senden.

So fügen Sie dem Schlüsselpaar einen neuen Benutzernamen oder eine neue E-Mail-Adresse hinzu

1. Öffnen Sie PGP Desktop und doppelklicken Sie auf den entsprechenden Schlüssel. Das Dialogfeld „Schlüssel-Info“ des ausgewählten Schlüssels wird angezeigt.
2. Klicken Sie auf **E-Mail-Adresse hinzufügen**. Das Dialogfeld „Namen hinzufügen“ wird angezeigt.
3. Geben Sie die neuen Informationen in die Felder **Vollständiger Name** und **E-Mail-Adresse** ein und klicken Sie auf **OK**. Sofern die Passphrase für den zu ändernden Schlüssel nicht zwischengespeichert ist, wird das Dialogfeld „PGP-Passphrase eingeben“ angezeigt.
4. Geben Sie die Passphrase für den privaten Teil des Schlüssels ein, den Sie ändern, und klicken Sie auf **OK**. Der neue Name wird am Ende der Liste mit den Benutzernamen hinzugefügt, die dem Schlüssel zugeordnet sind.

Hinweis: Wenn Sie Informationen im Schlüsselpaar ändern oder hinzufügen, müssen Sie das Schlüsselpaar immer mit dem Keyserver synchronisieren, damit stets Ihr aktueller Schlüssel verfügbar ist.

So löschen Sie einen Namen oder eine E-Mail-Adresse aus dem Schlüsselpaar

1. Klicken Sie in der Schlüsselliste auf das Pluszeichen links neben dem Schlüssel, um den Schlüssel zu erweitern.
2. Wählen Sie die Benutzer-ID aus, die Sie löschen möchten.
3. Drücken Sie die Entfernen-Taste auf der Tastatur. Ein Bestätigungsdialogfeld wird angezeigt.

Tipp: Sie können auch auf **Bearbeiten > Löschen** (Windows) oder auf **Bearbeiten > Entfernen** (Mac OS X) klicken.

4 Klicken Sie auf **Löschen**. Die Benutzer-ID wird gelöscht.

Schlüssel und X.509-Zertifikate importieren

Sie können öffentliche PGP-Schlüssel und Zertifikate vom Typ PKCS-12 X.509 (ein digitales Zertifikat, das von den meisten Webbrowsern verwendet wird) sowie öffentliche Zertifikate vom Typ PKCS-7 X.509 in Ihren PGP Desktop-Schlüsselbund importieren. Sie können auch X.509-Zertifikate im PEM-Format (Privacy Enhanced Mail) von Ihrem Browser importieren, indem Sie sie in Ihren öffentlichen Schlüsselbund kopieren.

Es gibt mehrere Methoden, den öffentlichen PGP-Schlüssel eines anderen Benutzers zu importieren und dem Schlüsselbund hinzuzufügen. Dies umfasst folgende Möglichkeiten:

- Doppelklicken Sie auf die Datei in Ihrem System. Falls PGP Desktop das Dateiformat erkennt, wird die Datei geöffnet und Sie werden aufgefordert, den Import der Schlüssel in der Datei zu bestätigen.
- Wählen Sie in PGP Desktop die Schlüsseldatei für den Import aus.
- Ziehen Sie die Datei mit dem öffentlichen Schlüssel in das Fenster von PGP Keys.

In S/MIME-E-Mail-Nachrichten enthaltene X.509-Zertifikate importieren

Wenn ein X.509-Zertifikat in einer S/MIME-E-Mail-Nachricht enthalten ist, die an Sie gesendet wurde, kann PGP Desktop die Zertifikate an den Schlüsselbund importieren. Auf diese Zertifikate werden dieselben Einstellungen angewendet, die Sie für gefundene öffentliche Schlüssel angegeben haben. Wenn dies entsprechend angegeben ist, extrahiert PGP Desktop das X.509-Zertifikat und importiert es dann an den Schlüsselbund. Wenn Sie E-Mail-Nachrichten mit importierten Zertifikaten verschlüsseln möchten, müssen Sie das Zertifikat manuell signieren.

Wenn Sie X.509-Zertifikate importieren möchten, wählen Sie **PGP > Einstellungen** und danach die Option **Schlüssel** aus. Wählen Sie dann die Option **Zum Speichern an eigenem Schlüsselbund auffordern** oder **Schlüssel an eigenem Schlüsselbund speichern** aus.

Passphrase ändern

Es empfiehlt sich, die Passphrase regelmäßig zu ändern, z. B. alle drei Monate. Noch wichtiger ist es, die Passphrase sofort zu ändern, wenn Sie vermuten, dass die Sicherheit gefährdet ist, z. B. wenn Ihnen jemand während der Eingabe über die Schulter geblickt hat.

Damit Sie die Passphrase eines geteilten Schlüssels ändern können, müssen Sie diesen zuerst wieder zusammenfügen.

Tipp: Wenn Sie die Passphrase des Schlüssels ändern, wird die Passphrase von Kopien des Schlüssels (z. B. Sicherungskopien) nicht geändert. Wenn Sie annehmen, dass die Passphrase nicht mehr geheim ist, empfiehlt die PGP Corporation, alle Sicherungskopien sicher zu löschen und neue Sicherungskopien des Schlüssels zu erstellen.

Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten und den SKM-Schlüsselmodus verwenden, können Sie die Passphrase des Schlüssels nicht ändern. SKM-Schlüssel werden durch eine auf Zufallsbasis erzeugte Passphrase geschützt (die wiederum selbst geschützt ist) und Sie werden nie aufgefordert, eine Passphrase für einen SKM-Schlüssel einzugeben. Informationen zum Ermitteln des Schlüsselmodus finden Sie unter *Schlüsselmodi* (auf Seite 132).

So ändern Sie die Passphrase des privaten Schlüssels

1. Öffnen Sie PGP Desktop und doppelklicken Sie auf den entsprechenden Schlüssel. Das Dialogfeld „Schlüssel-Info“ des ausgewählten Schlüssels wird angezeigt.
2. Klicken Sie auf **Passphrase ändern** und wählen Sie aus der Liste der angezeigten Befehle die Option **Passphrase ändern** **aus. Das** Dialogfeld „PGP-Passphrase eingeben“ wird angezeigt.
3. Geben Sie die *aktuelle* Passphrase für den privaten Schlüssel ein und klicken Sie auf **OK**. Das Dialogfeld „PGP-Passphrase bestätigen“ wird angezeigt.
4. Geben Sie die neue Passphrase in das erste Textfeld ein.
5. Geben Sie die Passphrase im Feld **Bestätigung** erneut ein.

   Die Passphrasen-Qualitätsanzeige kann als allgemeiner Anhaltspunkt für die Stärke der erstellten Passphrase verwendet werden. Dabei wird der Entropiewert der eingegebenen Passphrase mit einer echten zufälligen Zeichenkette mit 128 Bit verglichen. Dies entspricht dem Entropiewert eines AES-128-Schlüssels. Weitere Informationen finden Sie unter *Die Passphrasen-Qualitätsanzeige* (auf Seite 234).
6. Klicken Sie auf **OK**. Es wird ein Informationsdialogfeld mit der Meldung angezeigt, dass die Passphrase geändert wurde.

7 Klicken Sie auf **OK**. Die Passphrase wurde geändert.

Achtung: Wenn Sie die Passphrase ändern, weil Sie vermuten, dass sie in falsche Hände geraten ist, sollten Sie alle Sicherungsschlüsselbunde sicher löschen und eine Sicherungskopie des Schlüssels mit der neuen Passphrase erstellen.

Schlüssel, Benutzer-IDs und Signaturen löschen

PGP Desktop gibt Ihnen die Kontrolle über die Schlüssel an Ihren Schlüsselbunden sowie über die Benutzer-IDs und Signaturen an diesen Schlüsseln.

Bei öffentlichen Schlüsseln an Ihren Schlüsselbunden können Sie ganze Schlüssel, beliebige Benutzer-IDs an einem Schlüssel und beliebige oder alle Signaturen an einem Schlüssel löschen.

Bei Ihren Schlüsselpaaren können Sie ganze Schlüsselpaare oder beliebige Signaturen löschen. Sie können auch Benutzer-IDs aus einem Schlüsselpaar löschen, falls es sich nicht um die einzige Benutzer-ID des Schlüsselpaars handelt.

Beachten Sie jedoch, dass Sie die Benutzer-ID nicht aus einem Schlüssel löschen können, wenn es sich hierbei um die einzige Benutzer-ID handelt. Auch Autosignaturen können nicht von Schlüsseln gelöscht werden.

So löschen Sie einen Schlüssel vom PGP-Schlüsselbund

1 Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld **Schlüssel**. Alle Schlüssel am Schlüsselbund werden angezeigt.

2 Führen Sie einen der folgenden Schritte aus:

- Löschen Sie einen Schlüssel, indem Sie den Schlüssel auswählen und auf **Bearbeiten > Löschen** klicken. Klicken Sie im Bestätigungsdialogfeld auf **OK**. Der Schlüssel wird aus dem Schlüsselbund gelöscht.
- Löschen Sie eine Benutzer-ID (von einem öffentlichen Schlüssel) oder eine Signatur, indem Sie auf das Dreieck links neben dem Schlüssel mit der Benutzer-ID oder der Signatur klicken, die Sie löschen möchten. Dadurch werden die entsprechenden Benutzer-IDs und Signaturen angezeigt. Wenn Sie die Benutzer-ID oder Signatur gefunden haben, die Sie löschen möchten, klicken Sie auf die Benutzer-ID und dann auf **Bearbeiten > Löschen**. Klicken Sie im Bestätigungsdialogfeld auf **OK**. Die Benutzer-ID oder Signatur wird gelöscht.

  Beachten Sie, dass Sie Benutzer-IDs nicht von einem Schlüsselpaar löschen können.

Öffentliche Schlüssel deaktivieren und aktivieren

In bestimmten Situationen möchten Sie möglicherweise einen öffentlichen Schlüssel am Schlüsselbund vorübergehend deaktivieren. Dies trifft beispielsweise zu, wenn Sie einen öffentlichen Schlüssel zwar für die künftige Verwendung behalten möchten, der Schlüssel jedoch nicht bei jeder versendeten E-Mail-Nachricht in die Empfängerliste aufgenommen werden soll.

Es ist nicht möglich, Ihre Schlüsselpaare zu deaktivieren.

So deaktivieren Sie einen öffentlichen Schlüssel

1. Öffnen Sie PGP Desktop und klicken Sie auf das Element „Schlüssel“. Alle Schlüssel am Schlüsselbund werden angezeigt.
2. Doppelklicken Sie auf den öffentlichen Schlüssel, den Sie deaktivieren möchten. Das Dialogfeld „Schlüssel-Info“ des ausgewählten Schlüssels wird angezeigt.
3. Suchen Sie in den Schlüsseleigenschaften das Feld **Aktiviert**.
   - Wenn derzeit für die Einstellung **Aktiviert** die Option **Ja** ausgewählt ist, ist der Schlüssel aktiviert. Wenn Sie den Schlüssel deaktivieren möchten, klicken Sie einmal auf **Ja**. Im Feld **Aktiviert** wird jetzt die Option **Nein** angezeigt. Der Schlüssel ist deaktiviert.
   - Wenn derzeit für die Einstellung **Aktiviert** die Option **Nein** ausgewählt ist, ist der Schlüssel deaktiviert. Wenn Sie den Schlüssel aktivieren möchten, klicken Sie einmal auf **Nein**. Im Feld **Aktiviert** wird die Option **Ja** angezeigt. Der Schlüssel ist also aktiviert.

Ein deaktivierter Schlüssel kann nicht zum Verschlüsseln, Signieren, Entschlüsseln oder Verifizieren verwendet werden.

Tipp: Sie können Schlüssel an Ihrem Schlüsselbund auch mit dem PGP Universal Server synchronisieren. Diese Option wird in erster Linie zum Aktivieren bzw. Deaktivieren öffentlicher Schlüssel am Schlüsselbund verwendet. Klicken Sie hierzu mit der rechten Maustaste (oder bei gedrückter Ctrl-Taste) auf einen Schlüssel und wählen Sie **Synchronisieren** aus.

Einen öffentlichen Schlüssel verifizieren

Es ist schwer zu wissen, ob ein öffentlicher Schlüssel einer bestimmten Person gehört, sofern Sie den Schlüssel nicht direkt von der betreffenden Person auf einem Datenträger erhalten oder vom PGP Global Directory abrufen. Das Austauschen von Schlüsseln auf Datenträgern bietet sich in der Regel nicht an, besonders für Benutzer, die sich nicht am selben Ort befinden.

Daher stellt sich die Frage, wie sichergestellt werden kann, dass der öffentliche Schlüssel, der von einem öffentlichen Keyserver (nicht vom PGP Global Directory) abgerufen wurde, tatsächlich der öffentliche Schlüssel der Person ist, die auf dem Schlüssel aufgeführt ist? Die Lösung ist, dass Sie den Fingerabdruck des Schlüssels überprüfen müssen

Sie haben mehrere Möglichkeiten, den Fingerabdruck eines Schlüssels zu überprüfen. Es ist aber am sichersten, wenn Sie die Person anrufen und sich den Fingerabdruck am Telefon vorlesen lassen. Falls die Person nicht das Ziel eines Angriffs ist, ist es äußerst unwahrscheinlich, dass jemand dieses zufällige Gespräch abhört und sich als die Person ausgibt, die Sie am anderen Ende der Leitung erwarten. Sie können auch den Fingerabdruck auf Ihrer Kopie des öffentlichen Schlüssels einer Person mit dem Fingerabdruck des Originalschlüssels dieser Person auf einem öffentlichen Server vergleichen.

Der Fingerabdruck kann auf zwei Arten angezeigt werden: in einer eindeutigen Wortliste oder im Hexadezimal-Format.

So überprüfen Sie den digitalen Fingerabdruck auf einem öffentlichen Schlüssel

1. Öffnen Sie PGP Desktop und klicken Sie auf das Element „Schlüssel“. Alle Schlüssel am Schlüsselbund werden angezeigt.
2. Doppelklicken Sie auf den öffentlichen Schlüssel, dessen Fingerabdruck Sie prüfen möchten. Das Dialogfeld „Schlüssel-Info“ wird angezeigt.
3. Suchen Sie im zweiten Teil des Dialogfelds „Schlüssel-Info“ den digitalen Fingerabdruck.

   Klicken Sie bei Bedarf auf das Dreieck, damit es nach unten weist und der Fingerabdruck des Schlüssels angezeigt wird. Der Fingerabdruck wird entweder im Hexadezimal-Format (10 Gruppen zu je vier Zeichen) oder im Wortlistenformat (4 Spalten mit je fünf eindeutigen Wörtern) angezeigt.
4. Vergleichen Sie den Fingerabdruck auf dem Schlüssel mit dem Original-Fingerabdruck. Wenn beide Schlüssel übereinstimmen, handelt es sich um den echten Schlüssel. Andernfalls ist der Schlüssel wahrscheinlich nicht echt.

   Die Wortliste besteht aus bestimmten, von PGP Desktop verwendeten Authentifizierungswörtern. Die Wörter wurden sorgfältig ausgewählt, um phonetisch unterscheidbar und unmissverständlich zu sein. Die Wortliste erfüllt einen ähnlichen Zweck wie das Funkalphabet, mit dem Piloten Informationen über Funkkanäle mit Störgeräuschen übermitteln können.
5. Falls der Schlüssel gefälscht ist, löschen Sie ihn.
6. Öffnen Sie einen Webbrowser, rufen Sie das *PGP Global Directory* (*https://keyserver.pgp.com*) auf und suchen Sie nach dem echten öffentlichen Schlüssel.

Öffentliche Schlüssel signieren

Wenn Sie ein Schlüsselpaar erstellen, werden die Schlüssel automatisch signiert. Entsprechend können Sie den öffentlichen Schlüssel einer anderen Person signieren, wenn Sie sicher sind, dass es sich um den Schlüssel dieser Person handelt. Dadurch geben Sie an, dass Sie den Schlüssel verifiziert haben. Wenn Sie den öffentlichen Schlüssel einer Person signieren, wird der Schlüssel zusammen mit einem Signatursymbol und Ihrem Benutzernamen angezeigt.

Falls Sie ein Schlüsselpaar von einer Sicherungskopie oder von einem anderen Rechner importieren, muss dieses Schlüsselpaar signiert werden.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist die Schlüsselsignierung möglicherweise deaktiviert.

So signieren Sie einen Schlüssel

1. Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld **Schlüssel**. Alle Schlüssel am Schlüsselbund werden angezeigt.
2. Wählen Sie den Schlüssel aus, den Sie signieren möchten, und wählen Sie im Menü **Schlüssel** **die Option** **Signieren** aus. Das Dialogfeld „Schlüssel signieren“ wird geöffnet, wobei der Benutzername bzw. die E-Mail-Adresse und der Hexadezimal-Fingerabdruck im Textfeld angezeigt werden.

   Tipp: Sie können auch bei gedrückter Ctrl-Taste (bzw. bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste) auf den Schlüssel klicken. Wählen Sie im Kontextmenü die Option **Signieren** aus.
3. Wählen Sie unter **Mit Schlüssel signieren** den Schlüssel aus, mit dem Sie signieren möchten.
4. Damit die Signatur mit diesem Schlüssel exportiert werden kann, wählen Sie **Export der Signatur zulassen** aus.

   Eine exportierbare Signatur kann an Server gesendet werden und wird immer mit dem Schlüssel mitgesendet, wenn dieser exportiert wird. Durch die Aktivierung des Kontrollkästchens stimmen Sie dem Export Ihrer Signatur zu.
5. Vergewissern Sie sich im Feld **Zu signierende Elemente auswählen**, dass Sie den richtigen Schlüssel signieren.
6. Wenn Sie weitere Optionen wie Signaturtyp oder Ablaufdatum der Signatur konfigurieren möchten, klicken Sie auf **Optionen**.
7. Wählen Sie einen Signaturtyp **zum Signieren des öffentlichen Schlüssels aus. Folgende Optionen sind verfügbar:**

- **Nicht exportierbar**: Verwenden Sie diesen Signaturtyp, wenn der Schlüssel Ihrer Meinung nach gültig ist, Sie jedoch nicht möchten, dass sich andere Personen auf Ihre Zertifizierung verlassen. Dieser Signaturtyp kann nicht mit dem zugehörigen Schlüssel an einen Keyserver gesendet oder auf andere Art exportiert werden.
- **Exportierbar**: Verwenden Sie exportierbare Signaturen, wenn Ihre Signatur mit dem Schlüssel an den Keyserver gesendet wird, damit andere sich auf Ihre Signatur verlassen und daher Ihren Schlüsseln vertrauen können. Diese Vorgehensweise entspricht dem Aktivieren des Kontrollkästchens **Export der Signatur zulassen** im Menü **Schlüssel signieren**.
- **Meta-Vertrauensperson, nicht exportierbar**: Mit dieser Option wird bestätigt, dass dieser Schlüssel und alle Schlüssel, die durch diesen Schlüssel als Vertrauensperson signiert wurden, als Vertrauenspersonen akzeptiert wurden, die wiederum Schlüssel signieren können, die Sie automatisch als vertrauenswürdig einstufen. Dieser Signaturtyp ist nicht exportierbar.
- **Vertrauensperson, exportierbar**: Verwenden Sie diese Signatur, wenn Sie bestätigen möchten, dass dieser Schlüssel gültig ist und dass dem Besitzer des Schlüssels vollkommen vertraut werden soll, wenn dieser sich für andere Schlüssel verbürgt. Dieser Signaturtyp ist exportierbar. Sie können die Validierungsmöglichkeiten der Vertrauensperson auf eine bestimmte E-Mail-Domäne beschränken.

8 Wählen Sie im Feld **Ablaufdatum** **die Option** **Nie** aus, wenn diese Signatur nicht zu einem bestimmten Datum ablaufen soll. Legen Sie andernfalls ein Ablaufdatum fest.

9 Geben Sie im Feld **Erweitert** **eine maximale Vertrauenstiefe und eine Domäneneinschränkung ein:**

- Über die Option **Maximale Vertrauenstiefe** können Sie die Anzahl der Ebenen angeben, bis zu der Vertrauenspersonen verschachtelt werden können. Falls Sie beispielsweise den Wert 1 auswählen, kann nur eine Ebene von Vertrauenspersonen unter dem Schlüssel der Meta-Vertrauensperson liegen.
- Falls Sie die Möglichkeit für die Schlüsselvalidierung der Vertrauensperson auf eine einzige Domäne beschränken möchten, geben Sie den Domänennamen in das Textfeld **Domäneneinschränkung** ein.

10 Klicken Sie auf **Signieren**. Das Dialogfeld „PGP-Passphrase für Schlüssel eingeben“ wird angezeigt (falls die Passphrase nicht im Schlüsselanhänger gespeichert wurde).

11 Geben Sie bei Bedarf die Passphrase des Signaturschlüssels ein. Wenn die Passphrase zwischengespeichert wurde, werden Sie von PGP Desktop nicht zur Eingabe der Passphrase aufgefordert.

12 Klicken Sie auf **OK**. Der Schlüssel ist signiert.

Signaturen von öffentlichen Schlüsseln widerrufen

Unter Umständen kann es erforderlich oder wünschenswert sein, Ihre Signatur von einem Schlüssel am Schlüsselbund zu widerrufen.

▸ **So widerrufen Sie Ihre Signatur**

1. Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld **Schlüssel**. Alle Schlüssel am Schlüsselbund werden angezeigt.
2. Klicken Sie auf das Dreieck links neben dem Schlüssel, dessen Signatur Sie widerrufen möchten. Die Signaturen werden angezeigt.
3. Klicken Sie auf den Signaturschlüssel.
4. Klicken Sie auf **Bearbeiten > Widerrufen**. Ein Bestätigungsdialogfeld wird angezeigt.
5. Überprüfen Sie, ob die Schlüssel-ID und der Name des richtigen Schlüssels (von dem Sie die Signatur widerrufen möchten) angezeigt werden und klicken Sie auf **OK**. Das Dialogfeld „PGP-Passphrase für Schlüssel eingeben“ wird angezeigt.
6. Geben Sie die Passphrase ein und klicken Sie auf **OK**. Ihre Signatur des Schlüssels wird widerrufen.

Vertrauen für Schlüsselvalidierungen gewähren

Sie können nicht nur bestätigen, dass ein Schlüssel einer bestimmten Person gehört, sondern haben auch die Möglichkeit, dem Eigentümer des Schlüssels eine Vertrauensstufe zuzuweisen, die angibt, wie sehr Sie ihm in seiner Rolle als Vertrauensperson für Schlüssel anderer Personen vertrauen, die Sie in Zukunft erhalten mögen.

Dies bedeutet, dass jeder Schlüssel, den Sie erhalten, als gültig eingeschätzt wird, falls er von einer Person signiert wurde, die Sie als vertrauenswürdig bestätigt haben, selbst wenn Sie die Gültigkeit nicht selbst überprüft haben.

Sie müssen einen Schlüssel signieren, bevor Sie eine Vertrauensstufe dafür festlegen können.

Für öffentliche Schlüssel sind die Optionen **Keine**, **Marginal** und **Vertrauenswürdig** verfügbar. Vertrauenseinstellungen für Schlüsselpaare lauten **Keine** oder **Implizit** (d. h. dass es sich um Ihren eigenen Schlüssel handelt und Sie diesem vollständig vertrauen). Sie sollten nicht im Besitz von Schlüsselpaaren anderer Personen sein.

Weitere Informationen zu vertrauenswürdigen Schlüsseln finden Sie unter *Einführung in die Kryptografie*.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist die Möglichkeit, einen Schlüssel als vertrauenswürdig einzustufen, möglicherweise deaktiviert.

So stufen Sie einen Schlüssel als vertrauenswürdig ein

▸ **So stufen Sie einen Schlüssel als vertrauenswürdig ein**

1. Öffnen Sie PGP Desktop und klicken Sie auf das Element „Schlüssel". Alle Schlüssel am Schlüsselbund werden angezeigt.
2. Doppelklicken Sie auf den Schlüssel, den Sie als vertrauenswürdig einstufen möchten. Das Dialogfeld „Schlüssel-Info" wird angezeigt.
3. Klicken Sie im Bereich mit den **allgemeinen Informationen auf die aktuellen Einstellung für das Feld Vertrauen**. Ein Menü mit Vertrauenseinstellungen wird angezeigt.
4. Wählen Sie die gewünschten Einstellung aus.

Hinweis: Die Auswahl der Vertrauenseinstellung **Keine** oder **Marginal** bedeutet nicht, dass der Inhaber eines Schlüssels unehrlich oder nicht vertrauenswürdig ist. Sie bedeutet lediglich, dass *Sie nicht über ausreichende Informationen verfügen*, um die Echtheit eines Schlüsselinhabers oder einer Schlüsselquelle zu überprüfen.

Mit Unterschlüsseln arbeiten

Ein Schlüsselpaar von PGP Desktop besteht aus folgenden Elementen:

- Dem **Hauptschlüssel**, der nur zum Signieren verwendet wird
- Einem obligatorischen **Unterschlüssel für die Verschlüsselung**
- Einem oder mehreren *optionalen* **separaten Unterschlüsseln** zum Signieren, Verschlüsseln oder Signieren/Verschlüsseln

Der Hauptschlüssel wird standardmäßig zum Signieren verwendet, während ein Unterschlüssel immer zur Verschlüsselung verwendet wird. Dadurch kann die Sicherheit eines PGP Desktop-Schlüsselpaars verbessert werden, da ein separater Unterschlüssel für die Verschlüsselung widerrufen, entfernt oder einem PGP Desktop-Schlüsselpaar hinzugefügt werden kann, ohne Auswirkungen auf den Hauptschlüssel oder die darin enthaltenen Signaturen zu haben.

Neben dem Hauptschlüssel und dem obligatorischen Unterschlüssel für die Verschlüsselung können Sie zusätzliche Unterschlüssel für Ihr PGP Desktop-Schlüsselpaar erstellen. Sie können verschiedenste Kombinationen für Unterschlüssel erstellen, die nur zur Verschlüsselung, nur zum Signieren oder sowohl zum Verschlüsseln als auch zum Signieren verwendet werden können.

Zeigen Sie die Unterschlüssel eines Schlüsselpaars im Dialogfeld „Schlüsseleigenschaften“ an. In der Spalte „Verwendung“ wird die Funktion des Unterschlüssels angegeben:

Schlüssel	Beschreibung
	Unterschlüssel für die Verschlüsselung weisen ein blaues Schlosssymbol auf.
	Signatur-Unterschlüssel weisen ein blaues Stiftsymbol auf.
	Unterschlüssel, die sowohl zum Verschlüsseln als auch zum Signieren verwendet werden, weisen beide Symbole auf.
	Der standardmäßige Unterschlüssel für die Verschlüsselung weist oben links ein kleines grünes Häkchen auf.
	Der standardmäßige Signatur-Unterschlüssel weist oben links ein kleines grünes Häkchen auf.

Separate Unterschlüssel verwenden

Einige Beispiele für die sinnvolle Verwendung von zusätzlichen separaten Unterschlüsseln:

- **Mehrere Unterschlüssel**, die zur Verschlüsselung verwendet werden und in verschiedenen Phasen der Funktionsdauer eines Schlüsselpaars gültig sind, können einen Sicherheitsgewinn erreichen. Sie können für die Verschlüsselung Unterschlüssel erstellen, deren Start- und Ablaufdaten so gelegt sind, dass jeweils immer nur ein Unterschlüssel gilt. So können Sie beispielsweise mehrere Unterschlüssel erstellen, die jeweils nur für ein Jahr gelten. (Achten Sie dabei auf die Datumsübergänge.) Der Unterschlüssel für die Verschlüsselung wechselt dann jährlich. Dies kann eine nützliche Sicherheitsmaßnahme sein und bietet sich als automatisierte Methode zum regelmäßigen Wechseln des Unterschlüssels für die Verschlüsselung an, da dabei kein neuer öffentlicher Schlüssel erstellt und verteilt werden muss. Abgelaufene Unterschlüssel sind an einem Schlüsselsymbol mit einer roten Uhr zu erkennen.
- **Separate Signatur-Unterschlüssel** sind in Ländern und Regionen erforderlich, in denen separate Unterschlüssel für rechtsgültige digitale Signaturen vorgeschrieben sind.

Welche separaten Unterschlüssel Sie erstellen können, richtet sich nach dem Typ des Schlüsselpaars, mit dem Sie arbeiten:

- Für RSA-Schlüsselpaare können Sie Unterschlüssel allein zum Verschlüsseln, allein zum Signieren oder zum Verschlüsseln und Signieren erstellen.
- Für Diffie-Hellman/DSS-Schlüsselpaare können Sie Unterschlüssel allein zum Verschlüsseln oder allein zum Signieren erstellen, nicht jedoch zum kombinierten Verschlüsseln und Signieren.
- Unterschlüssel werden für ältere PGP-Legacy-Schlüsselpaare nicht unterstützt.

Unterschlüssel anzeigen

Sie können die Informationen zu den Unterschlüsseln auf Ihren Schlüsselpaaren anzeigen und ändern. Sie können jedoch nur die Informationen zu den Unterschlüsseln auf den öffentlichen Schlüsseln Ihres Schlüsselbunds anzeigen.

So zeigen Sie an, welche Unterschlüssel sich auf einem Schlüssel befinden

1. Öffnen Sie PGP Desktop und klicken Sie auf das Element „Schlüssel“. Alle Schlüssel am Schlüsselbund werden angezeigt.

2 Doppelklicken Sie auf den Schlüssel, dessen Eigenschaften Sie ermitteln möchten. Das Dialogfeld „Schlüsseleigenschaften“ wird für den ausgewählten Schlüssel angezeigt.

3 Klicken Sie auf das Dreieck links neben **Unterschlüssel**. Die Informationen zu den Unterschlüsseln für diesen Schlüssel werden angezeigt.

Neue Unterschlüssel erstellen

Wahrscheinlich werden Sie neue Unterschlüssel entsprechend der Anleitungen in diesem Abschnitt erstellen. Sie können Unterschlüssel jedoch auch bei der ersten Installation von PGP Desktop mit dem Assistenten für die Erstellung neuer Schlüssel erstellen. Weitere Informationen finden Sie unter *PGP Desktop erstmals verwenden* (auf Seite 16).

So erstellen Sie neue Unterschlüssel für ein Schlüsselpaar

1 Klicken Sie im Dialogfeld „Schlüsseleigenschaften“ im Bereich **Unterschlüssel** auf das Plussymbol. Das Dialogfeld „Neuer Unterschlüssel“ wird angezeigt.

2 Wählen Sie im Bereich **Diesen Unterschlüssel verwenden für** die Option **Verschlüsselung**, **Signieren** oder **Verschlüsselung und Signieren** aus. Die Auswahl hängt von der geplanten Verwendung des neuen Unterschlüssels ab.

3 Geben Sie im Feld **Schlüsselgröße** eine Schlüsselgröße zwischen 1024 und 4096 Bit ein.

4 Geben Sie im Feld **Startdatum** das Datum ein, an dem der neue Unterschlüssel in Kraft tritt.

5 Wählen Sie im Feld **Ablaufdatum** **die Option** **Nie** aus oder geben Sie ein Ablaufdatum an. Diese Angaben legen fest, wann der Unterschlüssel abläuft.

Hinweis: Damit es beim Verwalten mehrerer Unterschlüssel für das Schlüsselpaar nicht zu Verwirrungen kommt, sollten sich die Start- und Ablaufdaten der einzelnen Unterschlüssel nicht überschneiden.

6 Klicken Sie auf **Erstellen**. Das Passphrasen-Dialogfeld wird angezeigt.

7 Geben Sie die Passphrase ein und klicken Sie auf **OK**. Der Unterschlüssel wird erstellt.

Hinweis: Wenn Sie Informationen im Schlüsselpaar ändern oder hinzufügen, aktualisieren Sie das Schlüsselpaar auf dem Keyserver, damit stets Ihr aktueller Schlüssel verfügbar ist. Wählen Sie den Schlüssel in der Schlüsselliste aus, und klicken Sie im Menü **Schlüssel** **auf** **Auswahl aktualisieren**.

Schlüsselverwendung für Unterschlüssel festlegen

Jeder Unterschlüssel kann eigene Eigenschaften für die Schlüsselverwendung aufweisen. Zum Beispiel könnte ein Unterschlüssel nur für PGP Whole Disk Encryption und ein anderer für alle anderen Funktionen von PGP Desktop verwendet werden.

Es bietet sich beispielsweise an, die Schlüsselverwendung eines Schlüssels festzulegen, wenn Sie einen Schlüssel ausschließlich zur Laufwerksverschlüsselung und nicht zum Empfangen von verschlüsselten E-Mail-Nachrichten verwenden möchten. Wenn Sie einen öffentlichen Schlüssel verteilen, der PGP Messaging nicht zulässt, werden von einem anderen Benutzer gesendete E-Mail-Nachrichten nicht an Ihren öffentlichen Schlüssel verschlüsselt.

Hinweis: Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten und den SKM-Schlüsselmodus verwenden, können Sie keine Änderungen an den Markierungen für die Schlüsselverwendung vornehmen. Informationen zum Ermitteln des Schlüsselmodus finden Sie unter *Schlüsselmodi* (auf Seite 132).

So legen Sie die Schlüsselverwendung fest

1. Öffnen Sie PGP Desktop und klicken Sie auf das Element „Schlüssel“. Alle Schlüssel am Schlüsselbund werden angezeigt.

   Doppelklicken Sie auf den Schlüssel, dessen Eigenschaften Sie ermitteln möchten. Das Dialogfeld „Schlüsseleigenschaften“ wird für den ausgewählten Schlüssel angezeigt.
2. Klicken Sie im Dialogfeld „Schlüsseleigenschaften“ auf die Überschrift **Unterschlüssel**. Die Unterschlüssel für diesen Schlüssel werden angezeigt.
3. Doppelklicken Sie auf den Unterschlüssel, den Sie ändern möchten.
4. Klicken Sie auf den Pfeil neben der Option zum Bearbeiten der Unterschlüsselverwendung**. Die Verwendungseigenschaften für den Schlüssel werden angezeigt.**
5. Wählen Sie in der angezeigten Liste die PGP Desktop-Funktionen aus, für die dieser Schlüssel verwendet werden kann. Durch ein Häkchen neben dem Objekt wird angezeigt, dass der Schlüssel für diese Funktion verwendet werden kann.
6. Klicken Sie auf **Schließen**, um die Unterschlüsseleigenschaften zu speichern.
7. Klicken Sie erneut auf **Schließen**, um die Schlüsseleigenschaften zu speichern.

Unterschlüssel widerrufen

▸ **So widerrufen Sie einen Unterschlüssel**

1. Wählen Sie im Dialogfeld **Schlüsseleigenschaften** im Bereich **Unterschlüssel** den Unterschlüssel aus, den Sie widerrufen möchten.
2. Klicken Sie auf **Widerrufen** (Kreissymbol mit umgekehrtem Schrägstrich über der Liste der Unterschlüssel). Ein Bestätigungsdialogfeld wird angezeigt.
3. Klicken Sie auf **OK**, um den Unterschlüssel zu widerrufen. Das Passphrasen-Dialogfeld wird angezeigt.
4. Geben Sie die Passphrase ein und klicken Sie auf **OK**. Der Unterschlüssel wird widerrufen und das Symbol ändert sich in einen Schlüssel mit einem roten Kreissymbol mit einem Schrägstrich.

Unterschlüssel entfernen

▸ **So entfernen Sie einen Unterschlüssel**

1. Wählen Sie im Dialogfeld „Schlüsseleigenschaften“ im Bereich **Unterschlüssel** den Unterschlüssel aus, den Sie entfernen möchten.
2. Klicken Sie auf **Entfernen** (Minussymbol über der Liste mit den Unterschlüsseln). Ein Bestätigungsdialogfeld wird angezeigt.
3. Klicken Sie auf **OK**, um den Unterschlüssel zu entfernen. Der Unterschlüssel wird entfernt.

Mit ADKs arbeiten

Additional Decryption Keys (ADKs) sind Schlüssel, die von Sicherheitsbeauftragten in Organisationen zum Entschlüsseln von Nachrichten eingesetzt werden, die Mitarbeiter in der Organisation empfangen oder gesendet haben.

Nachrichten, die an einen Schlüssel mit einem ADK verschlüsselt sind, werden an den öffentlichen Schlüssel des Empfängers sowie an den ADK verschlüsselt. Der Inhaber des ADK kann die Nachricht also ebenfalls entschlüsseln.

ADK werden selten außerhalb einer von einem PGP Universal Server verwalteten Umgebung eingesetzt oder benötigt. Obwohl der PGP-Administrator im Regelfall keinen Bedarf für die Anwendung von Additional Decryption Keys hat, gibt es Umstände, die die Wiederherstellung der E-Mail-Nachrichten anderer Personen erforderlich machen. Dieser Fall kann z. B. eintreten, wenn ein Mitarbeiter längere Zeit krank ist oder wenn E-Mail-Aufzeichnungen auf behördliche Anordnung vorgelegt werden müssen und das Unternehmen E-Mail-Nachrichten für die Beweiserbringung in einem Gerichtsverfahren entschlüsseln muss.

Sie können nur ADKs an Ihren Schlüsselpaaren ändern.

ADKs zu einem Schlüsselpaar hinzufügen

So fügen Sie einem Schlüsselpaar einen ADK hinzu

1. Öffnen Sie PGP Desktop und klicken Sie auf das Element „Schlüssel“. Alle Schlüssel am Schlüsselbund werden angezeigt.
2. Doppelklicken Sie auf das Schlüsselpaar, dem Sie den ADK hinzufügen möchten. Das Dialogfeld „Schlüssel-Info“ des ausgewählten Schlüssels wird angezeigt.
3. Klicken Sie bei Bedarf auf das Dreieck links neben dem Bereich **Additional Decryption Keys (ADKs)**, sodass es nach unten weist. Die ADK-Informationen für diesen Schlüssel werden angezeigt, sofern sie konfiguriert wurden.
4. Klicken Sie rechts neben dem Bereich **Additional Decryption Keys (ADKs)** auf das Plussymbol.
5. Wählen Sie in der Liste den Schlüssel aus, den Sie als ADK verwenden möchten.
6. Klicken Sie auf **OK**. Das Dialogfeld „PGP-Passphrase für Schlüssel eingeben“ wird angezeigt.
7. Geben Sie die Passphrase für den Schlüssel ein, dem Sie den ADK hinzufügen möchten, und klicken Sie auf **OK**. Der ADK wird hinzugefügt.

Einen ADK aktualisieren

So aktualisieren Sie einen ADK

1. Wählen Sie den ADK, den Sie aktualisieren möchten, in der Liste der ADKs aus. Der ausgewählte ADK wird markiert.
2. Klicken Sie auf das Symbol mit dem Pfeil nach unten. Der ADK wird aktualisiert.

ADKs entfernen

So entfernen Sie einen ADK

1. Wählen Sie den ADK, den Sie entfernen möchten, in der Liste der ADKs aus. Der ausgewählte ADK wird markiert.
2. Klicken Sie auf das Minussymbol. In einer PGP-Warnung werden Sie aufgefordert, das Entfernen des ADK zu bestätigen.
3. Klicken Sie auf **OK**, um den ADK zu entfernen. Der ADK wird entfernt.

Mit Widerrufern arbeiten

Es kann vorkommen, dass Sie die Passphrase vergessen oder das Schlüsselpaar verlieren (falls beispielsweise Ihr Laptop gestohlen wird oder ein Festplattenfehler vorliegt).

Sofern Sie nicht die Schlüsselwiederherstellung verwenden, um den privaten Schlüssel wiederherzustellen, können Sie den Schlüssel nicht mehr verwenden und ihn auch nicht widerrufen, um anderen Personen anzuzeigen, dass er nicht mehr für die Verschlüsselung genutzt werden sollte. Als Schutzmaßnahme in derartigen Fällen können Sie eine Drittpartei als Schlüssel-Widerrufer einsetzen. Die von Ihnen eingesetzte Drittpartei kann den Schlüssel dann so widerrufen, als ob Sie ihn selbst widerrufen hätten.

Diese Funktion steht für Diffie-Hellman/DSS- und RSA-Schlüssel zur Verfügung.

Sie können nur die Widerrufer-Informationen Ihrer eigenen Schlüsselpaare ändern. Falls ein öffentlicher Schlüssel am Schlüsselbund einen Widerrufer aufweist, können Sie diese Informationen zwar einsehen, aber nicht ändern.

Designierte Widerrufer zu Schlüsseln hinzufügen

So fügen Sie einem Schlüssel einen designierten Widerrufer hinzu

1. Öffnen Sie PGP Desktop und wählen Sie unter dem Element „Schlüssel“ die Option **Eigene private Schlüssel** aus. Alle Schlüssel am Schlüsselbund werden angezeigt.
2. Doppelklicken Sie auf den Schlüssel, dem Sie einen Widerrufer hinzufügen möchten. Das Dialogfeld „Schlüssel-Info“ des ausgewählten Schlüssels wird angezeigt.
3. Klicken Sie rechts neben dem Bereich **Widerrufer** auf das Plussymbol. Das Dialogfeld „Schlüssel auswählen“ wird angezeigt.

4 Wählen Sie den Schlüssel aus, den Sie als Widerrufer-Schlüssel verwenden möchten, und klicken Sie auf **OK**. Sie werden in einem PGP-Warndialogfeld aufgefordert, das Hinzufügen der Widerrufer-Berechtigungen zu den ausgewählten Schlüsseln zu bestätigen.

5 Klicken Sie auf **Ja**, um fortzufahren, oder auf **Nein**, um abzubrechen. Das Dialogfeld „PGP-Passphrase für Schlüssel eingeben“ wird angezeigt.

6 Geben Sie die Passphrase für das Schlüsselpaar ein, dem Sie den Widerrufer hinzufügen, und klicken Sie auf **OK**. Das Dialogfeld „PGP-Informationen“ wird angezeigt.

7 Klicken Sie auf **OK**. Die ausgewählten Schlüssel sind jetzt zum Widerrufen des Schlüssels autorisiert. Zur effektiven Schlüsselverwaltung verteilen Sie eine aktuelle Kopie des Schlüssels an einen oder mehrere Widerrufer oder Sie laden den Schlüssel auf den Keyserver hoch.

Schlüssel widerrufen

Falls Sie Ihrem persönlichen Schlüsselpaar nicht mehr vertrauen sollten, können Sie den Schlüssel widerrufen. Dadurch teilen Sie allen Personen mit, dass sie Ihren öffentlichen Schlüssel nicht mehr verwenden sollten.

Sie können einen widerrufenen Schlüssel am besten verbreiten, indem Sie ihn auf einem öffentlichen Keyserver platzieren.

So widerrufen Sie einen Schlüssel

1 Öffnen Sie PGP Desktop und wählen Sie unter dem Element „Schlüssel“ die Option **Eigene private Schlüssel** aus. Alle Schlüssel am Schlüsselbund werden angezeigt.

2 Klicken Sie bei gedrückter Ctrl-Taste (oder bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste) auf den Schlüssel, den Sie widerrufen möchten.

3 Wählen Sie im Kontextmenü die Option **Widerrufen** aus. Im Dialogfeld „Widerrufen bestätigen“ werden Sie aufgefordert, das Widerrufen des Schlüssels zu bestätigen.

4 Klicken Sie auf **OK**, um das Widerrufen des ausgewählten Schlüssels zu bestätigen. Falls Sie den Vorgang abbrechen möchten, klicken Sie auf **Abbrechen**.

5 Geben Sie die Passphrase für das Schlüsselpaar ein, das Sie widerrufen, und klicken Sie auf **OK**. Ein widerrufener Schlüssel wird mit einem roten X gekennzeichnet, der angibt, dass der Schlüssel nicht mehr gültig ist.

6 Synchronisieren Sie den widerrufenen Schlüssel, damit alle Personen wissen, dass sie den nunmehr widerrufenen öffentlichen Schlüssel nicht mehr verwenden sollten.

Schlüssel teilen und wieder zusammenfügen

Mithilfe eines kryptografischen Vorgangs, der als Blakely-Shamir-Schlüsselteilung bekannt ist, können private Schlüssel auf mehrere Teilbesitzer aufgeteilt werden. Dieses Verfahren wird für Schlüssel mit extrem hohem Sicherheitsanspruch empfohlen.

Die PGP Corporation verwendet beispielsweise einen Unternehmensschlüssel, der auf mehrere Einzelpersonen aufgeteilt ist. Wenn der Schlüssel für die Signatur erforderlich ist, werden die Teile des Schlüssels vorübergehend wieder zusammengefügt.

Geteilte Schlüssel erstellen

Wenn Sie einen Schlüssel teilen, werden die Teile als Dateien gespeichert, die entweder an den öffentlichen Schlüssel eines Teilbesitzers verschlüsselt sind oder konventionell verschlüsselt sind, falls der Teilbesitzer nicht über einen öffentlichen Schlüssel verfügt. Nach der Schlüsselteilung wird bei jedem Signieren oder Entschlüsseln mit diesem Schlüssel automatisch versucht, den Schlüssel wieder zusammenzufügen.

So erstellen Sie einen geteilten Schlüssel

1. Öffnen Sie PGP Desktop und klicken Sie auf das Element „PGP Keys“. Alle Schlüssel am Schlüsselbund werden angezeigt.
2. Wählen Sie das Schlüsselpaar aus, das Sie teilen möchten. Das ausgewählte Schlüsselpaar wird hervorgehoben.
3. Klicken Sie auf **Schlüssel > Schlüssel teilen > Teilen**. Das Dialogfeld **Schlüssel teilen** wird angezeigt.
4. Fügen Sie Teilbesitzer für den geteilten Schlüssel hinzu, indem Sie deren Schlüssel in die Liste **Schlüssels/Benutzername** ziehen.
5. Wenn Sie einen Teilbesitzer hinzufügen möchten, der nicht über einen öffentlichen Schlüssel verfügt, *muss dieser Teilbesitzer physisch anwesend sein, um seine Passphrase einzugeben*. **Klicken Sie auf Hinzufügen**.
   - Lassen Sie den Teilbesitzer seine Passphrase zweimal eingeben und klicken Sie auf **OK**. In der Liste wird „Unbenannter Benutzer“ angezeigt.
   - Doppelklicken Sie auf „Unbenannter Benutzer“ und geben Sie einen beschreibenden Namen für die Person oder Organisation mit Teilen ein.

6 Geben Sie einen Speicherort für die Schlüsselteile an, indem Sie im Dialogfeld „Teiledatei-Zielordner“ auf **Durchsuchen** klicken und den gewünschten Speicherort auswählen.

7 Wenn alle Teilbesitzer aufgeführt sind, können Sie die Anzahl der Schlüsselteile angeben, die zum Entschlüsseln oder Signieren mit diesem Schlüssel erforderlich sein sollen.

   Standardmäßig ist jeder Teilbesitzer für einen Teil verantwortlich. Erhöhen Sie die Anzahl der Teile eines Teilbesitzers, indem Sie in der Spalte „Teile“ auf die Zahl doppelklicken und die neue Anzahl von Teilen eingeben.

8 Klicken Sie auf **Schlüssel teilen**. Das Dialogfeld „Schlüsselteilung bestätigen“ wird angezeigt.

9 Klicken Sie auf **OK**, um die Schlüsselteilung fortzusetzen. Der Passphrasen-Bildschirm wird angezeigt.

10 Geben Sie die Passphrase für den Schlüssel ein, der geteilt wird, und klicken Sie auf **OK**. Diese Passphrase muss eine Länge von mindestens sechs Zeichen aufweisen. Ein Bestätigungsdialogfeld wird geöffnet.

   Der Schlüssel wird geteilt und die Teile werden am angegebenen Speicherort gespeichert. Die Schlüsselteile werden mit den Namen der Teilbesitzer als Dateinamen und mit der Dateiendung `.shf` gespeichert.

11 Verteilen Sie die Schlüsselteile an die Besitzer und löschen Sie dann die lokalen Kopien der Teile.

Bewahren Sie den ursprünglichen Schlüssel, der geteilt wurde, sicher auf. Dieser Schlüssel ist erforderlich, um den geteilten Schlüssel für Entschlüsselungsfunktionen zusammenzufügen.

Geteilte Schlüssel wieder zusammenfügen

Nachdem ein Schlüssel auf mehrere Teilbesitzer aufgeteilt wurde, versucht PGP Desktop bei jedem Signieren oder Entschlüsseln mit diesem Schlüssel automatisch, den Schlüssel wieder zusammenzufügen. Es gibt zwei Möglichkeiten, den Schlüssel wieder zusammenzufügen: lokal und remote.

Beim lokalen Zusammenfügen von Schlüsselteilen muss der Teilbesitzer an dem Computer anwesend sein, an dem der Schlüssel zusammengefügt wird. Jeder Teilbesitzer muss die Passphrase für seinen Teil des Schlüssels eingeben.

Erfolgt das Zusammenfügen der Schlüsselteile remote, müssen die Remoteteilbesitzer ihre Schlüssel authentifizieren und entschlüsseln, bevor sie sie über das Netzwerk senden. Die TLS-Technologie (Transport Layer Security) von PGP Desktop stellt eine sichere Verbindung zum Übermitteln von Schlüsselteilen bereit, die es mehreren Einzelpersonen an räumlich getrennten Standorten ermöglicht, mit ihren Schlüsselteilen sicher zu signieren oder zu entschlüsseln.

Achtung: Bevor Schlüsselteile über das Netzwerk entgegengenommen werden, sollten Sie den Fingerabdruck jedes Teilbesitzers verifizieren und dessen öffentlichen Schlüssel signieren, um sicherzustellen, dass sein Authentifizierungsschlüssel legitim ist.

Vergewissern Sie sich bevor Sie beginnen, dass der ursprüngliche Schlüssel, der geteilt wurde, auf dem Computer vorhanden ist, an dem der Schlüssel zusammengefügt wird.

So fügen Sie einen geteilten Schlüssel wieder zusammen

1. Nehmen Sie mit jedem Teilbesitzer des geteilten Schlüssels Kontakt auf. Damit Schlüsselteile lokal zusammengefügt werden können, müssen die Teilbesitzer des Schlüssels anwesend sein.

   Damit Schlüsselteile über das Netzwerk gesammelt werden können, müssen Sie sicherstellen, dass die Remoteteilbesitzer PGP Desktop installiert haben und zum Senden ihrer Teiledatei des Schlüssel bereit sind. Die Remoteteilbesitzer benötigen Folgendes:

   - Ihre jeweiligen Schlüsselteiledateien und Passphrasen
   - Ein Schlüsselpaar (zur Authentifizierung an dem Computer, der die Schlüsselteile sammelt)
   - Eine Netzwerkverbindung
   - Die IP-Adresse oder den voll qualifizierten Domänennamen des Computers, der die Schlüsselteile sammelt

2. Wählen Sie auf dem Computer, an dem der Schlüssel zusammengefügt wird, im Finder die Datei(en) aus, die Sie mit dem geteilten Schlüssel signieren oder entschlüsseln möchten.
3. Halten Sie die Ctrl-Taste gedrückt und klicken Sie auf die Datei(en). Wählen Sie aus dem PGP-Kontextmenü die Option **Signieren oder entschlüsseln** aus. Das Dialogfeld „PGP-Passphrase für ausgewählten Schlüssel eingeben“ wird angezeigt, wobei der geteilte Schlüssel ausgewählt ist.
4. Klicken Sie auf **OK**, um den ausgewählten Schlüssel neu zu erstellen. Das Dialogfeld „Schlüsselteilsammlung“ wird angezeigt.
5. Führen Sie einen der folgenden Schritte aus:

   - Falls Sie die Schlüsselteile lokal sammeln, klicken Sie auf **Teiledatei auswählen** und suchen Sie dann nach den Teiledateien, die dem geteilten Schlüssel zugeordnet sind. Die Teiledateien können von der Festplatte, einem Wechseldatenträger oder einem aktivierten Laufwerk gesammelt werden. Fahren Sie mit dem nächsten Schritt fort.
   - Falls Sie Schlüsselteile über das Netzwerk sammeln, klicken Sie auf **Netzwerk starten**.

Das Passphrasen-Dialogfeld wird geöffnet. Wählen Sie im Feld **Signaturschlüssel** das Schlüsselpaar aus, das Sie zur Authentifizierung am Remotesystem verwenden möchten, und geben Sie die Passphrase ein. Klicken Sie auf **OK**, um den Computer auf den Empfang der Schlüsselteile vorzubereiten.

Der Status der Transaktion wird im Feld **Netzwerkteile** angezeigt. Wenn sich der Status in **Abhören** ändert, ist die PGP-Anwendung zum Empfangen der Schlüsselteile bereit.

Zu diesem Zeitpunkt müssen die Teilbesitzer ihre Schlüsselteile senden.

Wenn ein Schlüsselteil empfangen wird, wird der Bildschirm „Remoteauthentifizierung“ angezeigt. Falls Sie den Schlüssel, der zur Authentifizierung des Remotesystems verwendet wird, nicht signiert haben, wird der Schlüssel als ungültig angesehen. Obwohl Sie den geteilten Schlüssel auch mit einem ungültigen Authentifizierungsschlüssel wieder zusammenfügen können, wird dieses Vorgehen nicht empfohlen. Sie sollten den Fingerabdruck jedes Teilbesitzers prüfen und dessen öffentlichen Schlüssel signieren, um sicherzustellen, dass der Authentifizierungsschlüssel legitim ist.

6. Klicken Sie auf **Bestätigen**, um die Teiledatei anzunehmen.
7. Sammeln Sie weiterhin Schlüsselteile, bis im Dialogfeld „Schlüsselteilsammlung“ die Werte für „Insgesamt gesammelte Teile“ und „Insgesamt erforderliche Teile“ übereinstimmen.
8. Klicken Sie auf **OK**. Die Datei wird mit dem geteilten Schlüssel signiert oder entschlüsselt.

Vorgehensweise bei verloren gegangenen Schlüsseln oder Passphrasen

Wenn Sie Ihren Schlüssel verloren haben, können Sie ihn wiederherstellen, damit Sie weiterhin Daten verschlüsseln und entschlüsseln können. Die Vorgehensweise hierfür ist davon abhängig, ob Sie PGP Desktop als eigenständige Anwendung oder in einer von einem PGP Universal Server verwalteten Umgebung verwenden.

Wenn Sie die Passphrase vergessen haben, können Sie sie zurücksetzen. Dazu müssen Sie drei von fünf Sicherheitsfragen richtig beantworten, die Sie bei der Einrichtung des Schlüssels oder der Sicherheitsfragen beantwortet haben.

Schlüssel mit PGP Universal Server wiederherstellen

Dieser Abschnitt betrifft nur PGP Desktop-Benutzer in einer von einem PGP Universal Server verwalteten Umgebung, deren PGP-Administrator für die Installation von PGP Desktop eine Unterstützung zur Schlüsselwiederherstellung konfiguriert hat.

Falls Sie Ihren Schlüssel verlieren oder Ihre Passphrase vergessen und keine Sicherungskopie besitzen, von der Sie den Schlüssel wiederherstellen können, können Sie Informationen, die mit dem Schlüssel verschlüsselt wurden, nicht mehr entschlüsseln. Sie können den Schlüssel jedoch wiederherstellen, wenn der PGP-Administrator eine Richtlinie für die PGP-Schlüsselwiederherstellung für Sie implementiert hat. Dabei wird der Schlüssel verschlüsselt und so auf einem PGP Universal Server gespeichert, dass nur Sie ihn abrufen können.

Der PGP Universal Server, der die Schlüsselwiederherstellungsdaten besitzt, speichert Ihren Schlüssel so, dass nur Sie Zugriff auf ihn haben. Selbst der PGP-Administrator kann Ihren Schlüssel nicht entschlüsseln.

Falls der PGP-Administrator die Unterstützung für die Schlüsselwiederherstellung konfiguriert hat, werden Sie bei der Installation von PGP Desktop oder beim Erstellen von Sicherheitsfragen aufgefordert, zusätzliche „geheime“ Informationen einzugeben.

Sobald sich der Schlüssel auf dem Server befindet, können Sie ihn jederzeit wiederherstellen, indem Sie in PGP Desktop für Windows auf **Schlüssel > Ich habe meinen Schlüssel verloren** bzw. auf **Schlüssel > Ich habe meine Passphrase vergessen** oder in PGP Desktop für Mac OS X auf **Schlüssel > Wiederherstellen** klicken.

Tipp: Wenn Sie während der Installation von PGP Desktop nicht aufgefordert wurden, Ihre PGP-Fragen zu erstellen, und der PGP Universal Server-Administrator die lokale Schlüsselwiederherstellung zulässt, können Sie die Fragen manuell erstellen. Weitere Informationen finden Sie unter *Sicherheitsfragen erstellen* (auf Seite 91).

Schlüsselwiederherstellungsdaten erstellen

Beim Beantworten der PGP-Sicherheitsfragen erstellen Sie die Schlüsselwiederherstellungsdaten. In einer eigenständigen Umgebung werden diese Informationen auf der lokalen Festplatte in einer KRB-Datei gespeichert. In einer verwalteten Umgebung werden die Schlüsselwiederherstellungsdaten an den PGP Universal Server des Unternehmens gesendet, wenn Sie PGP Desktop installieren oder wenn Sie Ihren Schlüssel zurücksetzen.

Wählen Sie geheime persönliche Fragen mit Antworten aus, die Sie nicht vergessen werden. Die Fragen können bis zu 95 Zeichen umfassen. Eine gute Frage ist beispielsweise „Mit wem bin ich zum Strand gegangen?“ oder „Warum ist Fred weggegangen?“. Eine schlechte Frage wäre beispielsweise „Wie lautet der Mädchenname meiner Mutter?“ oder „Auf welches Gymnasium bin ich gegangen“.

Wenn Sie alle fünf PGP-Fragen erstellt und beantwortet haben, wird Ihr privater Schlüssel mithilfe der Blakely-Shamir-Schlüsselteilung in fünf Teile geteilt. Drei der fünf Teile sind für die Wiederherstellung des Schlüssels erforderlich. Die Teile werden dann mit dem Hash, der eindeutigen Identifizierungsnummer einer Antwort, verschlüsselt. Wenn Sie drei beliebige Antworten kennen, können Sie den gesamten Schlüssel erfolgreich wiederherstellen.

Sicherheitsfragen erstellen

Bevor Sie einen Schlüssel wiederherstellen oder eine neue Passphrase erstellen können, wenn Sie die alte vergessen haben, müssen Sie Sicherheitsfragen erstellen. Sie können die fünf Sicherheitsfragen anpassen, damit die Antworten ausschließlich Ihnen bekannt sind.

So erstellen Sie Sicherheitsfragen

1. Klicken Sie in PGP Desktop auf das Element „Schlüssel“ und wählen Sie Ihren Schlüssel aus.
2. Klicken Sie auf **Schlüssel > PGP-Fragen erstellen**. Der PGP-Sicherheitsfragenassistent wird angezeigt.
3. Wenn das Dialogfeld „Schlüsselwiederherstellung“ angezeigt wird, geben Sie in den Feldern für die Fragen fünf Fragen ein, die nur Sie beantworten können (die Standardfragen dienen lediglich als Beispiel).

Alice Cameron Security Question Assistant
Create Security Question 1 of 5
PGP Desktop requires you to answer a set of five questions about your life when recovering a forgotten passphrase or lost key. Consider your questions and answers carefully so that you can recall them in the future. Do not write them down.
Pick A Question
Who was the first person I ever had a crush on?
Personalize Your Question
Who was the first person I ever had a crush on?
Answer Your Question
Enter first and last name
Go Back
Continue

4 Klicken Sie im ersten Dialogfeld zum Erstellen der Sicherheitsfragen auf den Pfeil für das erste Feld, um die Frage auszuwählen, die Sie verwenden möchten. Beachten Sie, dass Sie Teile der Frage im nächsten Schritt anpassen können.

   Wenn Sie eine Frage eigenständig definieren möchten, klicken Sie auf **Geben Sie Ihre eigene Frage ein**.

5 Klicken Sie für die Option **Frage personalisieren** auf die Pfeile neben dem anpassbaren Text. Wenn Sie beispielsweise die erste Frage ausgewählt haben, können Sie die Frage anpassen, indem Sie „erste“ durch „zweite“ und „in die Sie verliebt waren“ durch „mit der Sie Händchen gehalten haben“ ersetzen.

   Wenn Sie eine eigene Frage erstellen, geben Sie die Frage in diesem Feld ein. Geben Sie eine Frage ein, auf die nur Sie die Antwort kennen.

6 Geben Sie unter **Antwort auf die Frage** die Antwort auf diese Sicherheitsfrage ein. Sie können die Antwort unter Beachtung von Groß- und Kleinschreibung eingeben. Wenn Sie die Frage beantworten, spielt diese jedoch keine Rolle.

   In diesem Feld wird ein Hinweis angezeigt, der ausgeblendet wird, sobald Sie mit der Eingabe der Antwort beginnen. Beispielweise wird für die Antwort auf die Frage „Wie hieß die erste Person, mit der Sie Händchen gehalten haben“ der Hinweis „Geben Sie den Vor- und Nachnamen ein“ angezeigt.

7 Wenn Sie die Frage festgelegt und die Antwort eingegeben haben, klicken Sie auf **Weiter**, um fortzufahren. Das Dialogfeld „Sicherheitsfrage 2 von 5 erstellen“ wird angezeigt.

8 Sie werden insgesamt zur Eingabe und Beantwortung von fünf Sicherheitsfragen aufgefordert. Wiederholen Sie die oben genannten Schritte, um eine Frage auszuwählen, anzupassen und zu beantworten.

9 Wenn Sie alle fünf Fragen und Antworten eingegeben haben, wird das Dialogfeld „PGP-Passphrase eingeben“ angezeigt.

10 Geben Sie die Passphrase des Schlüssels ein und klicken Sie auf **OK**.

11 Sie werden aufgefordert, die Schlüsselwiederherstellungsdatei zu speichern. Geben Sie den Namen und den Speicherort für die Datei ein und klicken Sie auf **Speichern**.

12 Klicken Sie auf **Fertig stellen**, um den Assistenten zu beenden.

Sie haben jetzt die fünf Sicherheitsfragen festgelegt. Wenn Sie Ihren Schlüssel verloren oder Ihre Passphrase vergessen haben, können Sie den Schlüssel wiederherstellen oder die Passphrase zurücksetzen, indem Sie mindestens drei der fünf Sicherheitsfragen richtig beantworten.

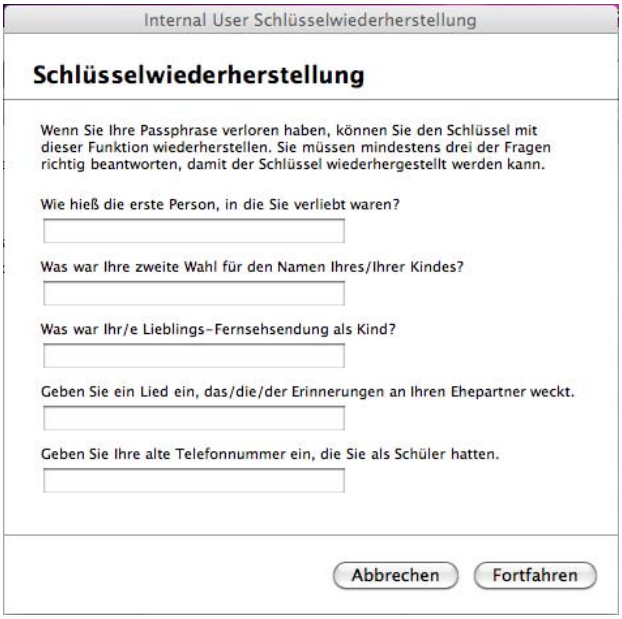
Schlüssel bei verloren gegangenen Schlüsseln bzw. Passphrasen wiederherstellen

Wenn Sie Ihren Schlüssel verloren oder die Passphrase vergessen haben, ist eine Wiederherstellung möglich, indem Sie den Schlüssel wiederherstellen. Dazu müssen Sie Sicherheitsfragen erstellt haben, die nur Sie beantworten können. Weitere Informationen finden Sie unter *Sicherheitsfragen erstellen* (auf Seite 91).

So stellen Sie Ihren Schlüssel wieder her

1. Klicken Sie in PGP Desktop auf das Element „Schlüssel“ und wählen Sie Ihren Schlüssel aus.
2. Klicken Sie auf **Schlüssel > Wiederherstellen**.
   - Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten, wird das Dialogfeld „Assistent für PGP-Passphrasen: Sicherheitsfragen beantworten“ angezeigt.
   - Wenn Sie in einer eigenständigen Umgebung arbeiten, wird das Dialogfeld „Datei mit Schlüsselwiederherstellungsdaten auswählen“ angezeigt. Wählen Sie die KRB-Datei aus, die Sie beim Erstellen der Sicherheitsfragen gespeichert haben, und klicken Sie auf **Öffnen**.

   Das Dialogfeld „Schlüsselwiederherstellung“ wird angezeigt.


Internal User Schlüsselwiederherstellung
Schlüsselwiederherstellung
Wenn Sie Ihre Passphrase verloren haben, können Sie den Schlüssel mit dieser Funktion wiederherstellen. Sie müssen mindestens drei der Fragen richtig beantworten, damit der Schlüssel wiederhergestellt werden kann.
Wie hieß die erste Person, in die Sie verliebt waren?
Was war Ihre zweite Wahl für den Namen Ihres/Ihrer Kindes?
Was war Ihr/e Lieblings-Fernsehsendung als Kind?
Geben Sie ein Lied ein, das/die/der Erinnerungen an Ihren Ehepartner weckt.
Geben Sie Ihre alte Telefonnummer ein, die Sie als Schüler hatten.
Abbrechen
Fortfahren

3. Beantworten Sie drei der fünf Sicherheitsfragen richtig und klicken Sie auf **Fortfahren**. Das Dialogfeld „PGP-Passphrase bestätigen“ wird angezeigt.
4. Geben Sie die neue Passphrase zwei Mal ein.

Wenn die Zeichen während der Eingabe der Passphrase angezeigt werden sollen, aktivieren Sie das Kontrollkästchen **Tastatureingabe anzeigen**. Stellen Sie sicher, dass niemand sehen kann, was Sie eingeben.

Die Passphrasen-Qualitätsanzeige kann als allgemeiner Anhaltspunkt für die Stärke der erstellten Passphrase verwendet werden. Dabei wird der Entropiewert der eingegebenen Passphrase mit einer echten zufälligen Zeichenkette mit 128 Bit verglichen. Dies entspricht dem Entropiewert eines AES-128-Schlüssels. Weitere Informationen finden Sie unter *Die Passphrasen-Qualitätsanzeige* (auf Seite 234).

5 Klicken Sie auf **OK**. Der Schlüssel wurde wiederhergestellt.

Schlüssel schützen

Sie sollten nicht nur Sicherungskopien Ihrer Schlüssel erstellen, sondern auch besonders sorgsam darauf achten, wo Sie den privaten Schlüssel aufbewahren. Obwohl der private Schlüssel durch eine Passphrase geschützt ist, die nur Sie kennen sollten, ist es möglich, dass eine andere Person Ihre Passphrase in Erfahrung bringt und Ihren privaten Schlüssel zum Entschlüsseln von E-Mail-Nachrichten oder zum Fälschen Ihrer digitalen Signatur verwendet. Jemand könnte Ihnen beispielsweise über die Schulter blicken und beobachten, welche Tastatureingaben Sie vornehmen, oder die Tastatureingaben über das Netzwerk oder sogar über das Internet abfangen.

Damit andere Personen, die Ihre Passphrase abgefangen haben, Ihren privaten Schlüssel nicht nutzen können, sollten Sie diesen ausschließlich auf Ihrem eigenen Computer speichern. Falls der Computer mit einem Netzwerk verbunden ist, stellen Sie sicher, dass Ihre Dateien nicht automatisch in eine systemweite Sicherung einbezogen werden, über die andere Personen Zugriff auf Ihren privaten Schlüssel erhalten könnten. Da ein Zugriff auf Computer in einem Netzwerk recht problemlos möglich ist, sollten Sie Ihren privaten Schlüssel auf einem Flash-Laufwerk speichern, falls Sie mit extrem vertraulichen Daten arbeiten. Dieses Laufwerk kann wie ein traditioneller Schlüssel immer dann angeschlossen werden, wenn Sie private Informationen lesen oder signieren möchten.

Als weitere Sicherheitsmaßnahme könnten Sie Ihrer privaten Schlüsselbunddatei einen anderen Namen zuweisen und sie nicht am Standardspeicherort speichern.

Ihre privaten und öffentlichen Schlüssel werden in getrennten Schlüsselbunddateien gespeichert. Sie können sie an einen anderen Speicherplatz auf der Festplatte oder auf einer Diskette kopieren. Standardmäßig werden der private Schlüsselbund (`secring.skr`) und der öffentliche Schlüsselbund (`pubring.pkr`) zusammen mit anderen Programmdateien im PGP-Ordner gespeichert. Sicherungskopien können an einem beliebigen Speicherort gespeichert werden.

Sie können PGP Desktop so konfigurieren, dass Schlüsselbunde automatisch nach dem Beenden von >prod< gesichert werden. Legen Sie die Sicherungsoptionen für Schlüsselbunde im Dialogfeld „Optionen“ auf der Registerkarte „Schlüssel“ (Windows) bzw. im Dialogfeld „Einstellungen“ (Mac OS X) fest.

Tipp: Wenn Sie die Passphrase des Schlüssels ändern, wird die Passphrase von Kopien des Schlüssels (z. B. Sicherungskopien) nicht geändert. Wenn Sie annehmen, dass die Passphrase nicht mehr geheim ist, empfiehlt die PGP Corporation, alle Sicherungskopien sicher zu löschen und neue Sicherungskopien des Schlüssels zu erstellen.

8 E-Mail-Nachrichten sichern

In diesem Abschnitt wird beschrieben, wie Sie E-Mail-Nachrichten automatisch und transparent mit PGP Desktop Email sichern.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat der PGP Universal Server-Administrator möglicherweise bestimmte Funktionen deaktiviert. Wenn eine Funktion deaktiviert wurde, wird das entsprechende Bedienelement auf der linken Seite nicht angezeigt und das Menü und andere Optionen für diese Funktion sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn der PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

E-Mail-Nachrichten mit PGP Desktop sichern 97
Offline-Richtlinien verwenden 102
Dienste und Richtlinien 103
Neue Sicherheitsrichtlinien erstellen 112
Mit der Sicherheitsrichtlinienliste arbeiten 123
PGP Desktop und SSL 130
Schlüsselmodi 132
PGP-Protokoll anzeigen 136
PGP-Skripte mit Entourage 2008 verwenden 137

E-Mail-Nachrichten mit PGP Desktop sichern

Wenn der Schutz von E-Mail-Nachrichten aktiviert ist, überwacht PGP Desktop den E-Mail-Verkehr zwischen dem E-Mail-Client und dem E-Mail-Server. PGP Desktop schaltet sich je nach Bedarf zu, um Nachrichten zu verschlüsseln, zu signieren, zu entschlüsseln oder zu verifizieren.

Nach der ordnungsgemäßen Konfiguration, die in der Regel von PGP Desktop automatisch durchgeführt wird, ist kein Eingriff Ihrerseits erforderlich, um ausgehende Nachrichten zu verschlüsseln und/oder zu signieren bzw. eingehende Nachrichten zu entschlüsseln und/oder zu verifizieren. Der Messaging-Proxy von PGP Desktop übernimmt diese Aufgaben für Sie.

Der Ablauf dieser Prozesse ist für eingehende und ausgehende Nachrichten unterschiedlich.

PGP Desktop überprüft automatisch alle eingehenden E-Mail-Nachrichten und führt die entsprechenden Aktionen aus (wie im folgenden Abschnitt beschrieben).

Bei ausgehenden Nachrichten kann PGP Desktop auf Basis der konfigurierten Richtlinien verschiedene Aktionen für Sie ausführen. Eine Richtlinie ist ein Satz von Anweisungen (z. B. „Wenn dies passiert, folgende Aktion durchführen"), mit denen PGP Desktop vorgeschrieben wird, wie in bestimmten Situationen vorzugehen ist. Durch die Kombination dieser Anweisungen lassen sich maßgeschneiderte Richtlinien für Ihre Anforderungen an die E-Mail-Sicherheit erstellen. PGP Desktop wird mit einem Satz vorkonfigurierter Richtlinien ausgeliefert, die dem Bedarf der meisten Benutzer gerecht werden. Dennoch behalten Sie die Kontrolle über alle Details dieser Richtlinien, falls Sie Änderungswünsche haben.

Wenn Sie PGP Desktop als eigenständige Lösung einsetzen und eine Nachricht senden, sucht PGP Desktop standardmäßig nach einem vertrauenswürdigen Schlüssel zum Verschlüsseln der Nachricht. Zunächst wird der Standardschlüsselring (unter Windows als „Alle Schlüssel" bezeichnet) oder der lokale Schlüsselbund (unter Mac OS X als „Schlüssel" bezeichnet) nach dem öffentlichen Schlüssel des Empfängers durchsucht. Wird der Schlüssel dort nicht gefunden, wird standardmäßig im PGP Global Directory nach einem vertrauenswürdigen Schlüssel für den Empfänger gesucht. Wenn dort kein vertrauenswürdiger Schlüssel zu finden ist, wird die Nachricht als Klartext gesendet, d. h. unverschlüsselt. Dieses standardmäßige Verhalten wird als *opportunistische Verschlüsselung* bezeichnet. Dabei handelt es sich um einen Kompromiss zwischen dem Schutz ausgehender Nachrichten und der Gewährleistung, dass die Nachrichten gesendet werden.

Informationen zum Erstellen neuer Richtlinien finden Sie unter *Neue Sicherheitsrichtlinien erstellen* (auf Seite 112).

Wenn Sie in einer mit PGP Universal geschützten Domäne arbeiten, bestimmen die lokalen PGP Desktop-Richtlinien, wie und wann Ihre Nachrichten verschlüsselt werden. Weitere Informationen erhalten Sie vom PGP Universal Server-Administrator Ihrer Organisation.

Eingehende Nachrichten

PGP Desktop entscheidet anhand des Nachrichteninhalts, wie mit einer eingehenden E-Mail-Nachricht vorgegangen wird. **Bei den folgenden Szenarien wird davon ausgegangen, dass PGP Desktop als eigenständige Lösung eingesetzt wird und nicht in einer von einen PGP Universal Server geschützten Domäne installiert ist** (bei einem PGP Universal Server werden u. U. E-Mail-Richtlinien angewendet, die vom PGP Universal Server-Administrator festgelegt wurden):

- **Die Nachricht ist weder verschlüsselt noch signiert.** Derartige Nachrichten werden von PGP Desktop ohne Überprüfung ihres Inhalts an den E-Mail-Client weitergeleitet.
- **Die Nachricht ist verschlüsselt, jedoch nicht signiert.** Wenn eine verschlüsselte Nachricht eingeht, versucht PGP Desktop, die Nachricht zu entschlüsseln. Zu diesem Zweck durchsucht PGP Desktop den lokalen Schlüsselbund nach dem privaten Schlüssel, mit dem die Nachricht entschlüsselt werden kann. Falls sich der private Schlüssel nicht am lokalen Schlüsselbund befindet, kann PGP Desktop die Nachricht nicht entschlüsseln und übergibt sie verschlüsselt an den E-Mail-Client. Ist der private Schlüssel am lokalen Schlüsselbund **vorhanden und die Passphrase ist für den privaten Schlüssel zwischengespeichert, wird die Nachricht sofort von PGP Desktop entschlüsselt. Ist die Passphrase nicht zwischengespeichert, werden Sie von PGP Desktop zur Eingabe der Passphrase aufgefordert. Sobald Sie die richtige Passphrase eingegeben haben, wird die Nachricht entschlüsselt. Nach dem Entschlüsseln der Nachricht übergibt PGP Desktop diese an den E-Mail-Client.**

  Wenn der Messaging-Proxy von PGP Desktop deaktiviert ist, kann PGP Desktop eingehende verschlüsselte Nachrichten nicht entschlüsseln. Die Nachrichten werden dann verschlüsselt an den E-Mail-Client weitergeleitet. Wenn Sie voraussichtlich verschlüsselte Nachrichten senden und empfangen werden, sollten Sie den Messaging-Proxy ständig aktiviert lassen. Der Proxy ist standardmäßig aktiviert.
- **Die Nachricht ist signiert, jedoch nicht verschlüsselt.** PGP Desktop durchsucht den lokalen Schlüsselbund nach einem öffentlichen Schlüssel, der zum Verifizieren der Signatur verwendet werden kann. Falls PGP Desktop den entsprechenden öffentlichen Schlüssel nicht am lokalen Schlüsselbund finden kann, sucht die Anwendung zunächst nach einem Keyserver unter „keys.domain" (wobei **domain** die Domäne des Nachrichtenabsenders bezeichnet), dann im *PGP Global Directory* (*https://keyserver.pgp.com*) und schließlich auf anderen konfigurierten Keyservern. Wenn PGP Desktop den richtigen öffentlichen Schlüssel an einem dieser Speicherorte findet, wird die Signatur verifiziert (bzw. nicht verifiziert, falls sie ungültig ist). Dann wird die Nachricht mit einer Anmerkung zur Signatur an den E-Mail-Client weitergeleitet. Die entsprechenden Angaben werden außerdem im PGP-Protokoll vermerkt. Kann PGP Desktop den entsprechenden öffentlichen Schlüssel nicht finden, wird die Nachricht ohne Verifizierung an den E-Mail-Client weitergeleitet.
- **Die Nachricht ist verschlüsselt und signiert.** PGP Desktop führt beide der oben beschriebenen Verfahren durch: Zunächst wird der private Schlüssel zum Entschlüsseln der Nachricht gesucht, dann der öffentliche Schlüssel zum Verifizieren der Signatur. Sollte eine Nachricht jedoch nicht entschlüsselt werden können, kann sie auch nicht verifiziert werden.

Falls PGP Desktop eine Nachricht weder entschlüsseln noch verifizieren kann, sollten Sie sich eventuell mit dem Absender der Nachricht in Verbindung setzen. Konnte die Nachricht nicht entschlüsselt werden, vergewissern Sie sich, dass der Absender Ihren echten öffentlichen Schlüssel verwendet hat. Falls die Nachricht nicht verifiziert werden konnte, bitten Sie den Absender, seinen Schlüssel im PGP Global Directory zu veröffentlichen. Ältere PGP-Versionen und andere OpenPGP-Produkte können auf die Webversion dieses Verzeichnisses unter *PGP Global Directory* (*https://keyserver.pgp.com*) zugreifen. Sie können den Absender auch bitten, seinen öffentlichen Schlüssel per E-Mail an Sie zu senden.

Hinweis: PGP Desktop verschlüsselt standardmäßig nur an Schlüssel, die als gültig bekannt sind. Wenn Sie keinen Schlüssel vom PGP Global Directory erhalten haben, müssen Sie u. U. den Fingerabdruck des Schlüssels mit dem Besitzer abgleichen und ihn signieren, damit Sie ihn verwenden können.

Informationen zu Anmerkungen für eingehende Nachrichten

Beim Empfang eingehender E-Mail-Nachrichten werden verschlüsselte Teile von PGP Desktop entschlüsselt und Signaturen verifiziert. Der verarbeiteten E-Mail-Nachricht wird dann ein als Anmerkung bezeichneter Textausschnitt hinzugefügt, der angibt, welche Verschlüsselung und welche Signaturen die Nachricht enthielt. Alle E-Mail-Nachrichten die zumindest teilweise geschützt waren (verschlüsselt, signiert oder beides) werden mit einer Anmerkung versehen. Wenn eine E-Mail-Nachricht ohne Schutz gesendet wurde (beispielsweise wurde die Nachricht vom Absender weder verschlüsselt noch signiert), wird ihr keine Anmerkung hinzugefügt.

Sie können zwischen drei Anmerkungsstufen wählen:

- **Maximal: Ausführliche Anmerkung:** In den Anmerkungen wird jede Aktion beschrieben, die von PGP Desktop während der Verarbeitung durchgeführt wurde.
- **Mittel: Fehler und Erfolg**: Dies ist die Standardoption. Es werden Anmerkungen hinzugefügt, wenn Verarbeitungsprobleme aufgetreten sind, z. B. unbekannte Schlüssel oder Signierer. Bei der Einstellung „Mittel“ werden allen entschlüsselten und/oder signierten E-Mail-Nachrichten Anmerkungen hinzugefügt, jedoch werden einzelne angehängte Dateien nicht aufgeführt.
- **Minimal: Nur Fehler:** Es werden nur Anmerkungen hinzugefügt, wenn Verarbeitungsprobleme aufgetreten sind, z. B. unbekannte Schlüssel oder Signierer.

Informationen zum Angeben der zu verwendenden Anmerkungsstufe finden Sie unter *Messaging-Optionen* (siehe "*Messaging-Einstellungen*" auf Seite 223).

In einer von einem PGP Universal Server verwalteten Umgebung hat der Administrator möglicherweise die Position der Anmerkung angegeben. Die Anmerkung kann den Nachrichtentext umschließen (Standardeinstellung) oder unter dem Nachrichtentext eingefügt werden.

Weitere Informationen zu Anmerkungen finden Sie im *PGP-Wissensdatenbankartikel 2039* (*http://support.pgp.com/?faq=2039*).

Ausgehende Nachrichten

Von Ihnen gesendete E-Mail-Nachrichten können verschlüsselt, signiert, verschlüsselt und signiert oder weder verschlüsselt noch signiert sein. Da Sie wahrscheinlich unterschiedliche Kombinationen für verschiedene Empfänger oder E-Mail-Domänen benötigen, müssen Sie für ausgehende E-Mail-Nachrichten Richtlinien für alle Möglichkeiten erstellen. Nachdem die gewünschten Richtlinien festgelegt wurden, werden Ihre E-Mail-Nachrichten automatisch und transparent geschützt.

Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten, werden Ihre PGP Desktop-Richtlinien durch die vom PGP Universal Server-Administrator festgelegten Richtlinien gesteuert. Möglicherweise hat der Administrator auch festgelegt, wie ausgehende E-Mail-Nachrichten gehandhabt werden sollen, wenn der PGP Universal Server nicht verfügbar ist. Diese Richtlinien werden als Offline-Richtlinien oder lokale Richtlinien bezeichnet.

Gesendete Objekte auf IMAP-E-Mail-Servern sichern

Wenn Sie einen IMAP-E-Mail-Server verwenden, werden Nachrichten im Ordner für gesendete Objekte in der Regel auf dem E-Mail-Server gespeichert. Die Kopie der gesendeten Nachricht wird von IMAP-E-Mail-Clients unter Verwendung des IMAP-Protokolls über das Netzwerk an den Ordner gesendet. Wenn die gesendete Nachricht nicht verschlüsselt ist, könnte sie abgefangen werden. PGP Desktop bietet Optionen zum Verschlüsseln und/oder Signieren von gesendeten Nachrichten bei ihrer Übertragung an den IMAP-Server.

In einer von einem PGP Universal Server verwalteten Umgebung hat der Administrator möglicherweise angegeben, dass alle Nachrichten im Ordner für gesendete Objekte gesichert werden müssen.

In einer eigenständigen Umgebung können Sie angeben, ob die gesendeten Nachrichten gesichert werden sollen. Wählen Sie dazu den Befehl **Extras > Optionen** (in PGP Desktop für Windows) bzw. **PGP > Einstellungen** (in PGP Desktop für Mac OS X) aus und klicken Sie auf die Registerkarte bzw. das Element „Messaging“. Geben Sie dann an, ob die Nachrichten verschlüsselt, verschlüsselt und signiert oder nur signiert werden sollen.

E-Mail-Nachrichten werden mit Ihrem öffentlichen PGP-Schlüssel verschlüsselt.

Wenn Sie auf den Ordner für gesendete Objekte zugreifen und die Passphrase des Schlüssels nicht zwischengespeichert ist, werden Sie zur Eingabe der Passphrase aufgefordert.

Wenn der Name des Ordners nicht von PGP Desktop erkannt wird (wenn der Ordner beispielsweise nicht „Gesendete Objekte“, sondern „Ausgehende Nachrichten“ heißt), werden Sie in einer Meldung gefragt, ob Ihre gesendeten Nachrichten gewöhnlich in diesem Ordner gespeichert werden. Beachten Sie, dass die erste in diesen Ordner kopierte Nachricht nicht verschlüsselt und/oder signiert ist. Nachfolgend in diesen Ordner kopierte Nachrichten werden jedoch verschlüsselt und/oder signiert.

Offline-Richtlinien verwenden

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, wird die Offline-Richtlinie für E-Mail-Nachrichten vom PGP Universal Server-Administrator festgelegt. Diese Richtlinie gibt an, wie E-Mail-Nachrichten gehandhabt werden, wenn der PGP Universal Server offline ist oder von PGP Desktop nicht erreicht werden kann.

- **Ausgehende Nachricht blockieren**: Ausgehende Nachrichten werden nicht gesendet. Wenn die Nachrichten vom E-Mail-Client in der Warteschlange gespeichert werden können, verbleiben sie in der Warteschlange, bis der PGP Universal Server verfügbar ist. Wenn die Nachrichten nicht in der Warteschlange gespeichert werden können, werden die E-Mail-Nachrichten blockiert.
- **Ausgehende Nachrichten als Klartext senden**: Sie werden gefragt, ob Sie die E-Mail-Nachricht ungesichert senden möchten. Wenn Sie die Nachricht senden möchten, wird sie als Klartext gesendet. Wenn Sie sie nicht senden möchten, wird die Nachricht blockiert.
- **Eigenständige Richtlinie befolgen**: PGP Desktop befolgt die eigenständige Richtlinie zur Verarbeitung Ihrer ausgehenden Nachrichten. Weitere Informationen finden Sie unter *Dienste und Richtlinien anzeigen* (auf Seite 104).

Weitere Informationen zu den Notifier-Meldungen, die Sie in den oben beschriebenen Fällen erhalten, finden Sie unter *PGP Desktop Notifier-Meldungen zu ausgehenden Nachrichten für Offline-Richtlinien* (auf Seite 35).

Der PGP Universal Server-Administrator kann festlegen, wie oft Ihre E-Mail-Richtlinien in PGP Desktop heruntergeladen werden. Wenn Sie sich im Offlinemodus befinden, bleibt die letzte heruntergeladene Offline-E-Mail-Richtlinie für die Verarbeitung der ausgehenden E-Mail-Nachrichten in Kraft. Wenn Sie sich für einen Zeitraum im Offlinemodus befinden, der länger ist als die für die Gültigkeit der eigenständigen Offline-E-Mail-Richtlinie zulässige Frist, hat der Administrator möglicherweise auch festgelegt, wie ausgehende E-Mail-Nachrichten verarbeitet werden sollen. In diesem Fall kann PGP Desktop damit beginnen, Ihre ausgehenden Nachrichten zu blockieren, oder dieselbe eigenständige Offline-E-Mail-Richtlinie kann für die Verarbeitung Ihrer ausgehenden Nachrichten verwendet werden (abhängig von der Definition der Richtlinie durch den Administrator).

Wenn Sie längere Zeit offline waren, können Sie manuell den Download von Richtlinien vom PGP Universal Server anfordern, wenn Sie wieder online sind. Wenn Sie wieder online sind, klicken Sie dazu in der Taskleiste auf das PGP Desktop-Symbol und wählen Sie die Option **Richtlinie aktualisieren** aus. Die aktuellsten Richtlinien werden vom PGP Universal Server heruntergeladen und alle Clientprotokolle werden auf den Server hochgeladen. Die Option zum manuellen Aktualisieren einer Richtlinie ist nur für verwaltete Benutzer verfügbar.

Wenn der PGP Universal Server-Administrator Ihnen die Verwendung von eigenständigen Richtlinien gestattet, finden Sie weitere Informationen unter *Neue Sicherheitsrichtlinien erstellen* (auf Seite 112).

Dienste und Richtlinien

Damit Sie Ihre ausgehenden Nachrichten mit PGP Desktop automatisch und transparent schützen können, müssen Sie zwei Begriffe kennen: Dienst und Richtlinie.

- **Dienst**: Informationen zu einem E-Mail-Konto auf dem System sowie zu den Richtlinien, die auf dieses Konto angewendet werden. In der Regel erstellt und konfiguriert PGP Desktop automatisch einen Dienst für jedes E-Mail-Konto auf dem System. In manchen Fällen sollten Sie einen Dienst manuell erstellen und konfigurieren.
- **Richtlinie**: Ein Satz von einer oder mehreren Anleitungen, die festlegen, welche Aktionen von PGP Desktop in bestimmten Situationen ausgeführt werden sollen. Richtlinien sind einem und oft auch mehreren Diensten zugeordnet (eine Richtlinie kann für verschiedene Dienste verwendet werden). Umgekehrt können einem Dienst mehrere Richtlinien zugewiesen werden, was auch oft der Fall ist.

Um festzulegen, wie eine bestimmte ausgehende E-Mail-Nachricht verarbeitet werden soll, überprüft PGP Desktop der Reihe nach (beginnend mit dem ersten Eintrag in der Liste) die Richtlinien, die für den jeweiligen Dienst konfiguriert wurden. Wenn eine entsprechende Richtlinie gefunden wird, werden die weiteren Richtlinien nicht überprüft. Stattdessen wird die gefundene Richtlinie angewendet.

Alle neuen Dienste werden mit den folgenden Standardrichtlinien erstellt:

- **Signier- und Verschlüsselungsschaltfläche**: Legt fest, dass E-Mail-Nachrichten sowohl signiert als auch verschlüsselt werden, wenn die Schaltflächen **Verschlüsseln** und **Signieren** in Microsoft Outlook 2002, 2003 oder 2007 aktiviert sind. Diese Richtlinie ist nur unter PGP Desktop für Windows verfügbar.
- **Signierschaltfläche**: Legt fest, dass E-Mail-Nachrichten signiert werden, wenn die Schaltfläche **Signieren** in Microsoft Outlook 2002, 2003 oder 2007 aktiviert ist. Diese Richtlinie ist nur unter PGP Desktop für Windows verfügbar.

- **Verschlüsselungsschaltfläche**: Legt fest, dass E-Mail-Nachrichten verschlüsselt werden, wenn die Schaltfläche **Verschlüsseln** in Microsoft Outlook 2002, 2003 oder 2007 aktiviert ist. Diese Richtlinie ist nur unter PGP Desktop für Windows verfügbar.
- **Adressenlisten-Administratoranforderungen**: Legt fest, dass Administratoranforderungen an Adressenlisten als Klartext gesendet werden, d. h. weder verschlüsselt noch signiert.
- **Adressenlisten-Sendevorgänge**: Legt fest, dass Sendevorgänge an Adressenlisten (für die Authentifizierung) signiert, jedoch nicht verschlüsselt gesendet werden.
- **Verschlüsselung erzwingen: [PGP] Vertraulich**: Legt fest, dass alle Nachrichten, die im E-Mail-Client als vertraulich gekennzeichnet sind oder den Text „[PGP]“ in der Betreffzeile enthalten, mit einem gültigen öffentlichen Schlüssel des Empfängers verschlüsselt werden **müssen**. Andernfalls können sie nicht gesendet werden.
- **Opportunistische Verschlüsselung**: Legt fest, dass alle Nachrichten, für die kein Verschlüsselungsschlüssel gefunden wird, unverschlüsselt (als Klartext) gesendet werden. Wenn diese Richtlinie als **letzte** Richtlinie in der Liste aufgeführt ist, wird sichergestellt, dass Nachrichten immer gesendet werden (wenn auch als Klartext), selbst wenn kein Schlüssel gefunden wird.

  Die Richtlinie „Opportunistische Verschlüsselung“ darf sich nur an letzter Stelle der Richtlinienliste befinden, da ihre Bedingungen immer zutreffen und PGP Desktop die Suche nach Richtlinien abbricht und die gefundene Richtlinie implementiert, sobald eine Übereinstimmung gefunden wird. Daher werden Richtlinien, die sich in der Liste unterhalb von „Opportunistische Verschlüsselung“ befinden, nie implementiert.

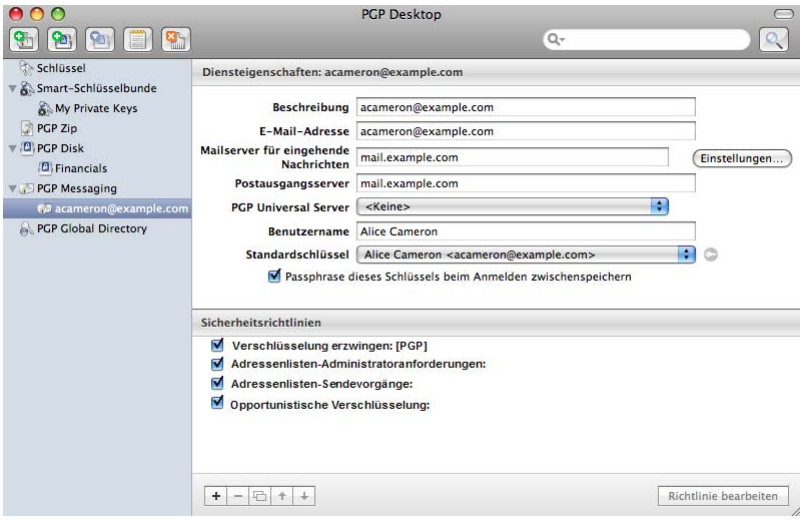
Hinweis: Die Standardrichtlinien können geändert, jedoch nicht gelöscht werden. Sie können allerdings deaktiviert und dann in der Richtlinienliste nach oben oder unten verschoben werden.

Dienste und Richtlinien anzeigen

So zeigen Sie Dienste und Richtlinien an

1. Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld „PGP Messaging“.
2. Klicken Sie auf den Namen des Dienstes, dessen Kontoeigenschaften Sie anzeigen möchten. Die Einstellungen für den ausgewählten Dienst werden im Arbeitsbereich von PGP Messaging angezeigt.

3 Wenn Sie die Details einer Richtlinie anzeigen möchten, klicken Sie unter **Sicherheitsrichtlinien** auf den Namen der Richtlinie, die Sie anzeigen möchten, und klicken Sie auf **Richtlinie anzeigen**. Die Einstellungen für die Richtlinie werden angezeigt. In diesem Abschnitt finden Sie Informationen darüber, welche Sicherheitsrichtlinie durchgesetzt wird. Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten, werden die Sicherheitsrichtlinien vom Administrator festgelegt.



Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, steht Ihnen ggf. die Option zum Überschreiben der Serverrichtlinien mit lokalen Richtlinien zur Verfügung. Wenn dies in einer Richtlinie angegeben ist, werden Ihre lokalen Richtlinien möglicherweise durchgesetzt, falls der PGP Universal Server aus irgendeinem Grund nicht zur Verfügung steht.

Neue Messaging-Dienste erstellen

Ein Dienst enthält Informationen zu einem E-Mail-Konto sowie zu den Sicherheitsrichtlinien, die auf ausgehende Nachrichten dieses E-Mail-Kontos angewendet werden sollen.

Wichtig: Gewöhnlich werden Dienste automatisch von PGP Desktop erstellt, wenn Sie Ihre E-Mail-Konten zum Senden oder Empfangen von Nachrichten verwenden. Wenn Sie selbst einen Dienst erstellen müssen, machen Sie sich zunächst mit den vorliegenden Anleitungen vertraut. Die fehlerhafte Konfiguration eines Dienstes führt u. U. zu Problemen beim Senden oder Empfangen von E-Mail-Nachrichten.

So erstellen Sie einen neuen Dienst

1 Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld „PGP Messaging“. Der PGP Messaging-Bildschirm wird angezeigt.

2 Klicken Sie auf **Neuen Dienst erstellen**. Sie können auch im Menü **Messaging** auf **Neuer Dienst** klicken. Der Bildschirm „Neuer Dienst“ wird angezeigt. Im Bereich **Diensteigenschaften** werden die Standardeinstellungen angezeigt, im Abschnitt „Sicherheitsrichtlinien“ werden die Standardsicherheitsrichtlinien angezeigt.

3 Geben Sie in das Feld **Beschreibung** einen aussagekräftigen Namen für den Dienst ein. (Dieser Schritt ist optional, kann sich jedoch bei der Verwendung mehrerer Dienste als hilfreich erweisen.)

4 Geben Sie in das Feld **E-Mail-Adresse** die diesem Dienst zugeordnete E-Mail-Adresse ein (z. B. acameron@beispiel.com).

5 Geben Sie den Namen des Posteingangs- und des Postausgangsservers ein oder klicken Sie auf **Servereinstellungen**, wenn Sie erweiterte Optionen festlegen möchten.

6 In diesem Fall wird das Dialogfeld „Servereinstellungen“ geöffnet.

Legen Sie die entsprechenden Einstellungen fest:

- **Servertyp**: Wählen Sie den Servertyp für den neuen Dienst aus:

  PGP Universal Server: Für Benutzer von PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung. Wenden Sie sich an den PGP-Administrator, wenn Sie weitere Informationen zu diesen Einstellungen benötigen. Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, wurden die richtigen Servereinstellungen automatisch heruntergeladen.

  Internet-E-Mail: Für Benutzer, die PGP Desktop als eigenständige Lösung mit einer POP- oder IMAP-Verbindung nutzen.

- **Name**: Geben Sie den Namen des E-Mail-Servers ein, der die *eingehenden* Nachrichten verarbeitet.

- **Protokoll**: Wählen Sie das Protokoll aus, das zum Abrufen von Nachrichten auf dem Mailserver für eingehende Nachrichten verwendet wird. Bei Auswahl der Einstellung **Automatisch** wird automatisch erkannt, ob es sich um eine POP- oder IMAP-Verbindung handelt.

- **Port**: Behalten Sie die Standardeinstellung **Automatisch** bei oder geben Sie einen Port an, über den die Verbindung zum Mailserver für eingehende Nachrichten hergestellt werden soll, um Nachrichten herunterzuladen (wenn Sie die Einstellungen **Internet-E-Mail** oder **PGP Universal** und dann entweder **POP** oder **IMAP** und nicht **Automatisch** ausgewählt haben).

- **SSL/TLS**: Geben Sie an, wie PGP Desktop mit dem E-Mail-Server kommunizieren soll:

- **Automatisch: Die PGP-Anwendung führt verschiedene Aktionen aus, um die Verbindung durch SSL/TLS zu schützen. Zunächst wird versucht, zum alternativen Port zu wechseln. Danach erfolgt ein Aufruf des Befehls „STARTTLS“ (sofern dieser vom Server unterstützt wird). Wenn keine dieser Vorgehensweisen erfolgreich ist, wird eine ungeschützte Verbindung zum Server hergestellt.**
- **STARTTLS erforderlich: PGP Desktop erfordert, dass der Server den Befehl „STARTTLS“ unterstützt.**
- **SSL erforderlich: PGP Desktop erfordert, dass der Server durch SSL geschützte Verbindungen zum angegebenen alternativen Port unterstützt.**
- **Nicht versuchen: PGP Desktop versucht nicht, die Verbindung zum E-Mail-Server durch SSL/TLS zu schützen.**
- **Bei SSL/TLS-Verbindungsversuch durch E-Mail-Client warnen: Wenn diese Option ausgewählt ist, zeigt PGP Desktop eine Warnung an, wenn der E-Mail-Client versucht, eine SSL/TLS-Verbindung aufzubauen, da dies den E-Mail-Proxyvorgang durch PGP Desktop verhindern würde. (Diese Option ist standardmäßig aktiviert.)**

Achtung: Diese Option darf nur aktiviert werden, wenn Sie sicher sind, dass der E-Mail-Server das SSL-Protokoll unterstützt. Auf diese Weise wird sichergestellt, dass PGP Desktop keine Nachrichten über ungeschützte Verbindungen sendet oder empfängt, falls beispielsweise ein Problem bei der Aushandlung des SSL-Protokolls für die Verbindung auftritt. **Wenn Sie diese Option aktivieren und der E-Mail-Server SSL nicht unterstützt, sendet oder empfängt PGP Desktop keine Nachrichten.**

- **Name**: Geben Sie den Namen des E-Mail-Servers ein, der die *ausgehenden* Nachrichten verarbeitet.
- **Port**: Übernehmen Sie die Einstellung **Automatisch (465, 25)** oder geben Sie einen anderen Port auf dem Postausgangsserver an, über den Nachrichten gesendet werden. Diese Option steht nur dann für den Postausgangsserver zur Verfügung, wenn die Einstellungen für den Mailserver für eingehende Nachrichten die Auswahl dieser Option zulassen.
- **SSL/TLS**: Geben Sie an, wie PGP Desktop mit dem E-Mail-Server kommunizieren soll:

  Automatisch: Die PGP-Anwendung führt verschiedene Aktionen aus, um die Verbindung durch SSL/TLS zu schützen. Zunächst wird versucht, zum alternativen Port zu wechseln. Danach erfolgt ein Aufruf des Befehls „STARTTLS“ (sofern dieser vom Server unterstützt wird). Wenn keine dieser Vorgehensweisen erfolgreich ist, wird eine ungeschützte Verbindung zum Server hergestellt.

STARTTLS erforderlich: PGP Desktop erfordert, dass der Server den Befehl „STARTTLS“ unterstützt.

SSL erforderlich: PGP Desktop erfordert, dass der Server durch SSL geschützte Verbindungen zum angegebenen alternativen Port unterstützt.

Nicht versuchen: PGP Desktop versucht nicht, die Verbindung zum E-Mail-Server durch SSL/TLS zu schützen.

- **Bei SSL/TLS-Verbindungsversuch durch E-Mail-Client warnen: Wenn diese Option ausgewählt ist, zeigt PGP Desktop eine Warnung an, wenn der E-Mail-Client versucht, eine SSL/TLS-Verbindung aufzubauen, da dies den E-Mail-Proxyvorgang durch PGP Desktop verhindern würde. (Diese Option ist standardmäßig aktiviert.)**

Hinweis: Informationen zum manuellen Herstellen einer Verbindung mit einem PGP Universal Server finden Sie unter *Manuelle Bindung an einen PGP Universal Server* (auf Seite 242).

Eigenschaften des Messaging-Dienstes bearbeiten

Achtung: Bevor Sie Änderungen an einem bestehenden Messaging-Dienst vornehmen, müssen Sie den E-Mail-Client beenden.

So ändern Sie die Kontoeigenschaften eines bestehenden Dienstes

1. Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld **PGP Messaging**.

   Klicken Sie auf den Namen des Dienstes, dessen Kontoeigenschaften Sie bearbeiten möchten. Die Einstellungen für den ausgewählten Dienst werden im Arbeitsbereich von PGP Messaging angezeigt.

2. Nehmen Sie die gewünschten Änderungen an den Kontoeigenschaften des Dienstes vor. Weitere Informationen finden Sie unter *Neue Messaging-Dienste erstellen* (auf Seite 105).

Dienste deaktivieren oder aktivieren

Wenn Sie einen Dienst nur anhalten, jedoch nicht löschen möchten, da Sie ihn möglicherweise wieder benötigen, können Sie ihn deaktivieren. Dies bietet sich an, wenn PGP Desktop nur Nachrichten von bestimmten Konten verarbeiten soll. Wenn Sie sicher sind, dass Sie den Dienst nicht mehr benötigen, können Sie den *Dienst löschen* (siehe "*Dienste löschen*" auf Seite 109).

So aktivieren oder deaktivieren Sie einen bestehenden Dienst

1. Wählen Sie unter „PGP Messaging“ den Namen des Dienstes aus, den Sie deaktivieren möchten. Die Einstellungen des Dienstes werden angezeigt. Vergewissern Sie sich, dass Sie den richtigen Dienst ausgewählt haben.
2. Führen Sie einen der folgenden Schritte aus:
   - Deaktivieren Sie den Dienst, indem Sie **Messaging > Dienst deaktivieren** auswählen. Der Dienst wird deaktiviert.
   - Aktivieren Sie den Dienst, indem Sie **Messaging > Dienst aktivieren** auswählen. Der Dienst wird aktiviert.

Tipp: Sie können auch bei gedrückter Ctrl-Taste (oder bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste) auf den Namen des Dienstes klicken und die Option zum Aktivieren bzw. Deaktivieren des Dienstes aus dem Kontextmenü auswählen.

Dienste löschen

Wenn Sie sicher sind, dass Sie einen Messaging-Dienst nicht mehr benötigen, können Sie diesen Dienst aus PGP Desktop löschen.

So löschen Sie einen Dienst

1. Wählen Sie unter „PGP Messaging“ den Namen des Dienstes aus, den Sie löschen möchten. Die Einstellungen des Dienstes werden angezeigt. Vergewissern Sie sich, dass Sie den richtigen Dienst ausgewählt haben.
2. Halten Sie die Ctrl-Taste gedrückt und klicken Sie auf den Namen des Dienstes (oder klicken Sie bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste darauf). Wählen Sie aus dem Kontextmenü die Option **Element entfernen** aus. Der Dienst wird gelöscht.

Mehrere Dienste

Einige E-Mail-Dienste und Internet-Dienstanbieter verwenden für einen einzelnen DNS-Namen mehrere E-Mail-Server, die der Reihe nach abgefragt werden. PGP Desktop kann in diesem Fall mehrere Messaging-Dienste für ein einzelnes E-Mail-Konto erstellen, da jeder E-Mail-Server getrennt betrachtet wird und somit seinen eigenen Messaging-Dienst erfordert.

PGP Desktop wird mit Platzhalterunterstützung für gängige E-Mail-Dienste ausgeliefert (z. B. *.yahoo.com und *.me.com bzw. *.mac.com). Falls Sie jedoch einen weniger gebräuchlichen E-Mail-Dienst verwenden oder sich die E-Mail-Server-Konfigurationen der Dienste ändern, könnte dieses Problem auftreten.

Wenn PGP Desktop mehrere Dienste für ein einzelnes E-Mail-Konto erstellt und Sie beim Überprüfen der Einstellungen feststellen, dass sich lediglich die E-Mail-Server unterscheiden (**mail1.beispiel.com für den ersten Dienst,** `mail2.beispiel.com` für den zweiten Dienst und `mail3.beispiel.com` für den dritten Dienst usw.), müssen Sie einen der Dienste möglicherweise manuell bearbeiten.

Die beste Lösung besteht darin, einen der Dienste manuell zu bearbeiten, sodass der E-Mail-Server-Eintrag für diesen Server mehrere E-Mail-Server unterstützen kann, die der Reihe nach abgefragt werden. Im oben aufgeführten Beispiel könnten Sie im Dialogfeld „Servereinstellungen“ den Servernamen für einen der Dienste in `mail*.beispiel.com` ändern und die anderen Dienste dann löschen.

Manche Konfigurationen können komplizierter sein und eine hiervon geringfügig abweichende Lösung erfordern. Wenn PGP Desktop beispielsweise Dienste mit den E-Mail-Servern pop.frodo.beispiel.com, smtp.bilbo.beispiel.com und mail.beispiel.com erstellen sollte, wäre die beste Platzhalterlösung ***.beispiel.com.**

Problembehebung bei PGP Messaging-Diensten

Standardmäßig ermittelt PGP Desktop automatisch die Einstellungen Ihres E-Mail-Kontos und erstellt einen PGP Messaging-Dienst, der als Proxy für den Messaging-Verkehr dieses Kontos dient.

Aufgrund der Vielzahl der möglichen E-Mail-Kontoeinstellungen und E-Mail-Server-Konfigurationen kann es jedoch vorkommen, dass ein von PGP Desktop automatisch eingerichteter Messaging-Dienst nicht ordnungsgemäß funktioniert.

Falls PGP Desktop einen Messaging-Dienst erstellt hat, der nicht Ihren Wünschen entspricht, können Sie das Problem möglicherweise anhand der folgenden Lösungsvorschläge beheben:

- Überprüfen Sie, ob eine Internetverbindung besteht und ob Sie E-Mail-Nachrichten senden und empfangen können, wenn PGP-Dienste angehalten wurden. Führen Sie dazu folgende Schritte aus:
  - Windows: Klicken Sie mit der rechten Maustaste auf das PGP Desktop-Symbol im Infobereich der Taskleiste und wählen Sie die Option **PGP-Dienste beenden** aus.
  - Mac OS X: Halten Sie die Wahltaste gedrückt und klicken Sie in der Menüleiste auf das PGP Desktop-Symbol. Wählen Sie die Option **Beenden** aus.

  Hinweis: Sie sollten den E-Mail-Client stets neu starten, wenn Sie die PGP-Dienste angehalten oder gestartet haben.
- Lesen Sie die Versionshinweise für die von Ihnen verwendete Version von PGP Desktop, um zu prüfen, ob es sich um ein bekanntes Problem handelt.

- Stellen Sie sicher, dass die SMTP-Authentifizierung für das E-Mail-Konto (in Ihrem E-Mail-Client) aktiviert ist. Dies wird empfohlen, damit PGP Desktop den Messaging-Verkehr über einen Proxy abwickeln kann. Wenn Sie nur über ein E-Mail-Konto verfügen und PGP Desktop nicht in einer von einem PGP Universal Server verwalteten Umgebung verwenden, ist keine SMTP-Authentifizierung erforderlich. Sie ist jedoch *erforderlich*, wenn Sie einen PGP Universal Server als SMTP-Server verwenden oder wenn Sie mehrere E-Mail-Konten auf dem gleichen SMTP-Server haben.
- Überprüfen Sie das PGP-Protokoll auf Einträge, die Hinweise auf die Art des Problems enthalten.
- Falls SSL/TLS im E-Mail-Client aktiviert ist und PGP Desktop den Messaging-Verkehr über einen Proxy abwickeln soll, müssen Sie die Option deaktivieren. (Der Schutz der Verbindung zwischen dem E-Mail-Client und dem E-Mail-Server wird dadurch *nicht* aufgehoben. PGP Desktop versucht standardmäßig automatisch, für jede ungeschützte Verbindung den SSL/TLS-Schutz zu aktivieren. Der E-Mail-Server muss SSL/TLS unterstützen, damit die Verbindung geschützt werden kann.)
- Wenn entweder **STARTTLS erfordern** oder **SSL erfordern** (in den SSL-/TLS-Einstellungen des Dialogfelds „Servereinstellungen“) ausgewählt ist, *muss* der E-Mail-Server SSL/TLS unterstützen. Andernfalls werden von PGP Desktop keine Nachrichten gesendet oder empfangen.
- Wenn das E-Mail-Konto keine Standard-Portnummern verwendet, stellen Sie sicher, dass diese Ports in den Einstellungen des Messaging-Dienstes enthalten sind.
- Falls PGP Desktop mehrere Messaging-Dienste für ein E-Mail-Konto erstellt, verwenden Sie einen Platzhalter für den Namen des E-Mail-Servers. Weitere Informationen finden Sie unter *Mehrere Dienste* (auf Seite 109).
- Löschen Sie den PGP Messaging-Dienst, der nicht ordnungsgemäß funktioniert, und senden und empfangen Sie E-Mail-Nachrichten. Der Messaging-Dienst wird von PGP Desktop neu erstellt.

Falls das Problem durch keine dieser Maßnahmen behoben werden kann, versuchen Sie Folgendes:

1. Löschen Sie den PGP Messaging-Dienst, der nicht ordnungsgemäß funktioniert.
2. Halten Sie alle PGP Desktop-Dienste an und beenden Sie PGP Desktop. So halten Sie die Dienste an
   - Windows: Klicken Sie mit der rechten Maustaste auf das PGP Desktop-Symbol im Infobereich der Taskleiste und wählen Sie die Option **PGP-Dienste beenden** aus.
   - Mac OS X: Halten Sie die Wahltaste gedrückt und klicken Sie in der Menüleiste auf das PGP Desktop-Symbol. Wählen Sie die Option **Beenden** aus.

3 Überprüfen Sie, ob eine Internetverbindung besteht und ob Sie E-Mail-Nachrichten senden und empfangen können, wenn PGP-Dienste angehalten wurden.

4 Öffnen Sie den E-Mail-Client und notieren Sie sich die Einstellungen des E-Mail-Kontos (einschließlich Benutzername, E-Mail-Adresse, Posteingangs- und Postausgangsserver, Protokoll des Posteingangsservers sowie alle E-Mail-Server-Ports, die nicht die Standardwerte verwenden).

5 Schließen Sie den E-Mail-Client und starten Sie PGP Desktop neu. Dadurch werden die PGP-Dienste neu gestartet:

- Windows: Starten Sie entweder den Computer neu oder öffnen Sie PGP Desktop über das Windows-Startmenü.
- Mac OS X: Starten Sie entweder den Computer neu oder öffnen Sie PGP Desktop.

6 Erstellen Sie anhand der zuvor notierten Kontoeinstellungen manuell einen PGP Messaging-Dienst.

7 Öffnen Sie den E-Mail-Client und senden und empfangen Sie E-Mail-Nachrichten.

8 Falls weiterhin Probleme mit einem PGP Messaging-Dienst auftreten, stehen folgende Informationsquellen zur Verfügung:

- *Website der PGP Corporation* (*http://www.pgp.com*)
- *PGP-Supportwebsite* (*https://support.pgp.com*)
- *PGP-Supportforen* (*http://forum.pgp.com*)

Neue Sicherheitsrichtlinien erstellen

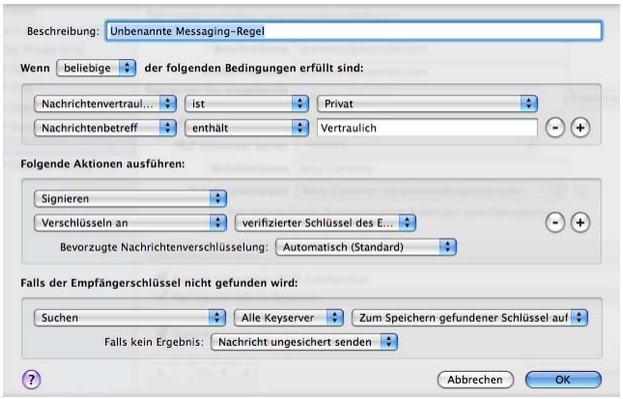
Mit Sicherheitsrichtlinien wird gesteuert, wie ausgehende E-Mail-Nachrichten von PGP Desktop gehandhabt werden.

Hinweis: Wenn Sie eine neue Sicherheitsrichtlinie erstellen, wird eine Messaging-Sicherheitsrichtlinie und keine Adressenlisten-Richtlinie erstellt. Sie können keine neuen Adressenlisten-Richtlinien erstellen, Sie können jedoch die Standardrichtlinien für Adressenlisten bearbeiten.

So erstellen Sie eine neue Sicherheitsrichtlinie

1 Klicken Sie im Bedienfeld „PGP Messaging“ auf den Namen des Dienstes, für den Sie eine neue Sicherheitsrichtlinie erstellen möchten. Die Einstellungen für den Dienst werden zusammen mit der Liste der vorhandenen Sicherheitsrichtlinien angezeigt.

2 Klicken Sie unten im Bildschirm auf das Plussymbol. Das Dialogfeld „Unbenannte Messaging-Regel“ wird angezeigt.


Beschreibung: Unbenannte Messaging-Regel
Wenn beliebige der folgenden Bedingungen erfüllt sind:
Nachrichtenvertraul... ist Privat
Nachrichtenbetreff enthält Vertraulich
Folgende Aktionen ausführen:
Signieren
Verschlüsseln an verifizierter Schlüssel des E...
Bevorzugte Nachrichtenverschlüsselung: Automatisch (Standard)
Falls der Empfängerschlüssel nicht gefunden wird:
Suchen Alle Keyserver Zum Speichern gefundener Schlüssel auf
Falls kein Ergebnis: Nachricht ungesichert senden
Abbrechen
OK

Wenn Ihre E-Mail-Domäne von einem PGP Universal Server geschützt ist, werden für die Richtlinieneinstellungen des Servers möglicherweise andere Felder als in der Abbildung angezeigt.

3 Geben Sie in das Feld **Beschreibung** einen aussagekräftigen Namen für die neue Richtlinie ein, die Sie erstellen.

4 Wählen Sie im ersten Abschnitt mit den Richtlinienbedingungen im Feld **Falls** eine der folgenden Optionen:

- **Falls beliebige**: Die Richtlinie wird angewendet, wenn eine der Bedingungen erfüllt ist.
- **Falls alle**: Die Richtlinie wird nur angewendet, wenn alle Bedingungen erfüllt sind.
- **Falls keine**: Die Richtlinie wird nur angewendet, wenn keine der Bedingungen erfüllt ist.

5 Wählen Sie im ersten Bedingungsfeld Folgendes aus:

- **Empfänger**: Die Richtlinie wird nur auf Nachrichten an den angegebenen Empfänger angewendet.
- **Empfängerdomäne**: Die Richtlinie wird nur auf E-Mail-Nachrichten in der angegebenen Empfängerdomäne angewendet.
- **Absender: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Absenderadresse angewendet.**
- **Nachricht: Die Richtlinie wird nur auf Nachrichten mit dem angegebenen Signierungs- und/oder Verschlüsselungsstatus angewendet.**
- **Nachrichtenbetreff**: Die Richtlinie wird nur auf Nachrichten mit dem angegebenen Nachrichtenbetreff angewendet.

- **Nachrichtenkopf**: Die Richtlinie wird nur auf Nachrichten angewendet, bei denen die angegebene Kopfzeile die festgelegten Kriterien erfüllt. Beachten Sie, dass die im nächsten Abschnitt beschriebenen Bedingungen (ist, ist nicht, enthält usw.) für den Text gelten, der in das Textfeld eingegeben wird, das nach Auswahl von **Nachrichtenkopf** angezeigt wird.

Hinweis: Bei der Suche nach Nachrichtenköpfen in MAPI-E-Mail-Systemen können Sie nur nach den Kopfzeilen für Betreff, Vertraulichkeit, Priorität und Wichtigkeit suchen.

- **Nachrichtentext**: Die Richtlinie wird nur auf Nachrichten mit dem angegebenen Nachrichtentext angewendet.
- **Nachrichtengröße: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Größe (in Byte) angewendet.**
- **Nachrichtenpriorität**: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Nachrichtenpriorität angewendet.
- **Nachrichtenvertraulichkeit**: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Nachrichtenvertraulichkeit angewendet.

6 Wählen Sie im zweiten Bedingungsfeld Folgendes aus:

- **ist**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *übereinstimmt*.
- **ist nicht**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *nicht übereinstimmt*.
- **enthält**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld den Text im Textfeld *enthält*.
- **enthält nicht**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld den Text im Textfeld *nicht enthält*.
- **beginnt mit**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *beginnt*.
- **endet mit**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *endet*.
- **stimmt mit Muster überein**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Textmuster im Textfeld *übereinstimmt*.
- **ist größer als**: Die Bedingung ist erfüllt, wenn die Nachrichtengröße *größer ist als* der im Textfeld eingegebene Text.
- **ist kleiner als:** Die Bedingung ist erfüllt, wenn die Nachrichtengröße *kleiner ist als* der im Textfeld eingegebene Text.

7 Wählen Sie im dritten Bedingungsfeld Folgendes aus:

- **Texteingabefeld**: Geben Sie den Text für die Übereinstimmungskriterien ein. Wenn Sie beispielsweise **Nachrichtengröße ist größer als** ausgewählt haben, geben Sie eine Zahl für die Größe der Nachricht ein.
- **normal**: Das Übereinstimmungskriterium für die Nachrichtenvertraulichkeit ist *normal*.
- **keine** bzw. **normal**: Das Übereinstimmungskriterium für die Nachrichtenvertraulichkeit ist *keine* (Mac OS X) bzw. *normal* (Windows).
- **persönlich**: Das Übereinstimmungskriterium für die Nachrichtenvertraulichkeit ist *persönlich*.
- **privat**: Das Übereinstimmungskriterium für die Nachrichtenvertraulichkeit ist *privat*.
- **vertraulich**: Das Übereinstimmungskriterium für die Nachrichtenvertraulichkeit ist *vertraulich*.
- **signiert**: Das Übereinstimmungskriterium für die Nachricht ist „signiert".
- **verschlüsselt**: Das Übereinstimmungskriterium für die Nachricht ist „verschlüsselt".
- **verschlüsselt an Schlüssel-ID**: Das Übereinstimmungskriterium für „verschlüsselt an Schlüssel-ID" (Sie müssen dann eine Schlüssel-ID in das angezeigte Textfeld eingeben).
- **niedrig**: Das Übereinstimmungskriterium für die Nachrichtenpriorität ist *niedrig*.
- **normal**: Das Übereinstimmungskriterium für die Nachrichtenpriorität ist *normal*.
- **hoch**: Das Übereinstimmungskriterium für die Nachrichtenpriorität ist *hoch*.

Erstellen Sie weitere Bedingungszeilen, indem Sie auf das Pluszeichen klicken.

8 Wählen Sie im Bereich **Für die Nachricht folgende Aktionen ausführen** im ersten Aktionsfeld Folgendes aus:

- **Klartext senden**: Gibt an, dass die Nachricht als Klartext gesendet werden soll, d. h. weder signiert noch verschlüsselt.
- **Signieren**: Gibt an, dass die Nachricht signiert werden soll.
- **Verschlüsseln an**: Gibt an, dass die Nachricht verschlüsselt werden soll.

9 Wählen Sie im zweiten Aktionsfeld Folgendes aus:

- **verifizierten Schlüssel des Empfängers**: Gewährleistet, dass die Nachricht nur an einen verifizierten Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann.

- **nicht verifizierten Schlüssel des Empfängers**: Ermöglicht, dass die Nachricht an einen nicht verifizierten Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann. Führt auch eine Verschlüsselung an einen möglicherweise vorhandenen verifizierten Schlüssel durch.
- **verifizierten End-to-End-Schlüssel des Empfängers**: Gewährleistet, dass die Nachricht nur an einen verifizierten End-to-End-Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann. Ein End-to-End-Schlüssel befindet sich im alleinigen Besitz des jeweiligen Empfängers. In einer von einem PGP Universal Server verwalteten Umgebung ist dies ein CKM-Schlüssel (Client Key Mode). Im Gegensatz dazu befindet sich ein SKM-Schlüssel (Server Key Mode) im Besitz des PGP Universal Servers.

  Ob es sich um einen End-to-End-Schlüssel handelt, wird unter Windows im Dialogfeld „Schlüsseleigenschaften" und unter Mac OS X im Dialogfeld „Schlüssel-Info" im Feld **Gruppe** angezeigt. **Nein** bedeutet, dass es ein End-to-End-Schlüssel (d. h. nicht Teil einer Gruppe) *ist*, und **Ja** bedeutet, dass es sich *nicht* um einen End-to-End-Schlüssel handelt.
- **nicht verifizierten End-to-End-Schlüssel des Empfängers**: Ermöglicht, dass die Nachricht an einen nicht verifizierten End-to-End-Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann. Führt auch eine Verschlüsselung an einen möglicherweise vorhandenen verifizierten Schlüssel durch.
- **eine Liste von Schlüsseln**: Gibt an, dass die Nachricht nur an Schlüssel in der Liste verschlüsselt werden kann.

Erstellen Sie weitere Aktionszeilen, indem Sie auf das Pluszeichen klicken.

10 Wählen Sie im Feld **Bevorz. Verschlüsselung** Folgendes aus:

- **Automatisch**: Das Nachrichtenverschlüsselungsformat wird von PGP Desktop ausgewählt. Dies ist die empfohlene Einstellung. Wählen Sie nur dann eine andere Option aus, wenn Sie genau wissen, warum Sie eines der anderen Nachrichtenverschlüsselungsformate benötigen.
- **PGP-partitioniert**: Legt „PGP-partitioniert" als bevorzugtes Nachrichtenverschlüsselungsformat fest. Dieses Format gewährleistet die größte Rückwärtskompatibilität mit älteren PGP- und OpenPGP-Produkten.
- **PGP/MIME**: Legt „PGP/MIME" als bevorzugtes Nachrichtenverschlüsselungsformat fest. Mit PGP/MIME kann die gesamte Nachricht, einschließlich Anlagen, in einem Durchgang verschlüsselt und signiert werden, was schneller ist und zu einer besseren Wiedergabe der gesamten Nachricht führt.
- **S/MIME**: Legt „S/MIME" als bevorzugtes Nachrichtenverschlüsselungsformat fest. Wählen Sie „S/MIME" aus, wenn Sie dieses Format verwenden müssen, obwohl der Benutzer über einen PGP-Schlüssel verfügt.

11 Wählen Sie im Bereich **Falls der Schlüssel des Empfängers nicht verfügbar ist** (bzw. unter Mac OS X im Bereich **Falls der Empfängerschlüssel nicht gefunden wird**) im ersten Feld **Folgendes aus:**

- **keys.domain durchsuchen und: Gibt an, dass die Suche sowohl in keys.domain als auch auf einem anderen, von Ihnen angegebenen Server durchgeführt wird.**
- **Suchen**: Ermöglicht die Suche nach einem entsprechenden Schlüssel, wenn am lokalen Schlüsselbund kein Schlüssel gefunden wird.
- **Nachricht als Klartext signieren: Gibt an, dass die Nachricht als Klartext gesendet werden soll, jedoch signiert wird.**
- **Nachricht ungesichert senden: Gibt an, dass die Nachricht als Klartext gesendet werden soll.**
- **Nachricht blockieren**: Gibt an, dass die Nachricht nicht gesendet werden soll, wenn kein entsprechender Schlüssel gefunden wird.

12 Wählen Sie im zweiten Feld **Schlüssel nicht gefunden** Folgendes aus:

- **Alle Keyserver**: Gibt an, dass alle Keyserver, einschließlich des PGP Global Directory, nach einem entsprechenden Schlüssel durchsucht werden sollen.
- **PGP Global Directory bzw. keyserver.pgp.com**: Gibt an, dass nur das PGP Global Directory durchsucht wird.
- **[konfigurierte Keyserver]**: Gibt an, dass nur der Keyserver durchsucht wird, den Sie aus der Liste der aktuell konfigurierten Keyserver auswählen. Beachten Sie, dass andere Keyserver als das PGP Global Directory möglicherweise nicht verifizierte Schlüssel bereitstellen. Diese können nicht verwendet werden, wenn laut Richtlinie verifizierte Schlüssel erforderlich sind. Sofern Sie nicht genau wissen, warum ein bestimmter anderer Keyserver durchsucht werden soll, und Sie darauf vorbereitet sind, diese Schlüssel bei Bedarf manuell zum Verifizieren zu suchen, sollten Sie nur das PGP Global Directory durchsuchen. Diese Option ist nur unter Windows verfügbar.
- **Keyserver-Liste bearbeiten**: Ermöglicht Ihnen das Hinzufügen von Keyservern zur Liste der aktuell konfigurierten Keyserver. Diese Option ist nur unter Windows verfügbar.

13 Geben Sie im letzten Feld **Schlüssel nicht gefunden** Folgendes an:

- **Gefundene Schlüssel zwischenspeichern**: Gibt an, dass ein gefundener Schlüssel zwischengespeichert werden soll. Die Schlüssel in diesem Zwischenspeicher werden automatisch zum Verifizieren signierter Nachrichten verwendet. Wenn Sie verifiziert wurden, werden Sie für die Verschlüsselung genutzt.
- **Zum Speichern gefundener Schlüssel auffordern**: Gibt an, dass PGP Desktop anfragen soll, ob Sie einen bestimmten gefundenen Schlüssel am lokalen Schlüsselbund speichern möchten.

- **Gefundene Schlüssel speichern**: Gibt an, dass gefundene Schlüssel automatisch am lokalen Schlüsselbund gespeichert werden sollen.

14 Wählen Sie in der Liste **Falls kein Ergebnis** Folgendes aus:

- **Nachricht als Klartext signieren: Ermöglicht, dass Nachrichten, für die kein Verschlüsselungsschlüssel gefunden wird, signiert und als Klartext gesendet werden.**
- **Nachricht ungesichert senden: Die Nachricht wird nicht verschlüsselt.**
- **Nachricht blockieren: Verhindert, dass Nachrichten gesendet werden, für die kein Verschlüsselungsschlüssel gefunden wurde.**

15 Klicken Sie auf **OK**, wenn Sie alle Richtlinieneinstellungen konfiguriert haben. Die neue Richtlinie wird in der Liste der Sicherheitsrichtlinien angezeigt.

Reguläre Ausdrücke in Richtlinien

PGP Desktop unterstützt bei der Eingabe von Sicherheitsrichtlinien in Textfeldern die Verwendung von regulären Ausdrücken. Mit regulären Ausdrücken erzielen Sie über eine einzige Textzeichenfolge Übereinstimmungen mit mehreren Textzeichenfolgen.

Hinweis: Zusätzlich zu den folgenden Beispielen unterstützt PGP Desktop auch weitergehende reguläre Ausdrücke, die sich an Standardformaten orientieren. Das Kriterium „stimmt mit Muster überein“ bedeutet, dass der Suchbegriff mit einem regulären Ausdruck übereinstimmt.

Für einige Bedingungen von E-Mail-Richtlinien ist es erforderlich, dass ein Teil einer E-Mail-Nachricht mit einem Muster übereinstimmt. Die Muster in der Bedingung haben die Form eines regulären Ausdrucks. Ein regulärer Ausdruck ist eine Zeichenfolge, die das Format für einen Begriff darstellt, der übereinstimmen muss. Jeder Begriff, der dem Format des regulären Ausdrucks entspricht, ist eine Übereinstimmung.

Im Folgenden sind einige allgemeine Elemente von regulären Ausdrücken aufgeführt:

?	Gibt an, dass es eine oder keine Instanz des vorherigen Ausdrucks geben sollte.
+	Gibt an, dass es mindestens eine Instanz des vorherigen Ausdrucks gibt.
.	Entspricht einem beliebigen Einzelzeichen.
*	Gibt an, dass es keine, eine oder eine beliebige Anzahl von Instanzen des vorherigen Ausdrucks geben sollte.
[ ]	Entspricht einem beliebigen Einzelzeichen, das in der Klammer

	angegeben ist.
`[a-z]`	Entspricht einem kleingeschriebenen Buchstaben von a bis z.
`[1-9]`	Entspricht einer Ziffer von 1 bis 9.
`{n}`	Eine Folge von genau n Übereinstimmungen des Ausdrucks.

Im Folgenden sind Beispiele für reguläre Ausdrücke aufgeführt, die mit gebräuchlichen Objekten übereinstimmen, die in einer vertraulichen E-Mail-Nachricht enthalten sein können.

Daten	Beispiel	Regulärer Ausdruck
Telefonnummer	(555)555-4567	\(?[2-9][0-9]{2}[\)-.][2-9][0-9]{2}[-.][0-9]{4}
E-Mail-Adresse	joe@beispiel.com	[a-zA-Z0-9._%-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,6}
Kreditkartennummer	1234 1234 1234 1234	[1-9][0-9]{3} ?[0-9]{4} ?[0-9]{4} ?[0-9]{4}
Sozialversicherungsnummer	123-45-6789	[0-9]{3}-[0-9]{2}-[0-9]{4}
Ort, Abkürzung des Bundeslands	München, BY	.*, [A-Z][A-Z][A-Z]
Aus 1 bis 3 Zeichen bestehende Abkürzung des Bundeslands	BY	[A-Z][A-Z][A-Z]
Postleitzahl	12345	[0-9]{5}(-[0-9]{4})?
Eurobeträge mit vorangestelltem €-Zeichen	$3.95	\$[0-9]+.[0-9][0-9]
Datum, numerisch	2003-08-06	[0-9]{4}-[0-9]{2}-[0-9]{2}
Datum, alphanumerisch	3. Januar 2003	(Januar|Februar|März|April|Mai|Juni|Juli|August|September|Oktober|November|Dezember)\.?(3[0-1]|[1-2][0-9]|0?[0-9]), [0-9]{4}
HTTP-URL	http://www.beispiel.com	https?://(([012][0-9]{0,2}\.){3}[012][0-9]{0,2}|([a-zA-Z0-9]+\.)+[a-zA-Z0-9]{2,6})(/.*)?
IP-Adresse	123.123.123.123	([012][0-9]{0,2}\.){3}[012][0-

Daten	Beispiel	Regulärer Ausdruck
		9]{0,2}
Leerzeile		^$

Informationen und Beispiele zu Sicherheitsrichtlinien

Wenn Sie einen Dienst erstellen, werden automatisch mehrere Sicherheitsrichtlinien erstellt:

- Verschlüsselung erzwingen: [PGP] Vertraulich
- Signier- und Verschlüsselungsschaltfläche*
- Signierschaltfläche*
- Verschlüsselungsschaltfläche*
- Adressenlisten-Administratoranforderungen
- Adressenlisten-Sendevorgänge
- Opportunistische Verschlüsselung:

** Diese Richtlinien sind nur in PGP Desktop für Windows verfügbar.*

Die Reihenfolge der Standardrichtlinienregeln ist wichtig. Achten Sie darauf, dass die oben beschriebene Reihenfolge genau eingehalten wird.

In diesem Abschnitt wird die Funktionsweise der Standardsicherheitsrichtlinien beschrieben. Darüber hinaus werden zwei Beispielsituationen beschrieben, für die Sie eine Sicherheitsrichtlinie erstellen könnten, sowie deren Konfiguration.

Hinweis: Wenn Sie Änderungen an den Standardrichtlinien vornehmen und die Standardeinstellungen wiederherstellen möchten, klicken Sie im Dialogfeld „Nachrichtenrichtlinie“ auf **Standard wiederherstellen** (Windows) oder auf **Zurücksetzen** (Mac OS X).

Standardrichtlinie „Opportunistische Verschlüsselung“

„Opportunistische Verschlüsselung“ ist eine der Standardsicherheitsrichtlinien, die von PGP Desktop automatisch für einen Dienst erstellt werden. Es gibt folgende Einstellungen für diese Standardrichtlinie:

- Falls: beliebige
- Bedingungen: Empfängerdomäne / ist / *
- Aktionen: Signieren / Verschlüsseln an / verifizierten Schlüssel des Empfängers
- Bevorzugte Verschlüsselung: Automatisch

- Schlüssel nicht gefunden: keys.domain durchsuchen und / keyserver.pgp.com / Gefundene Schlüssel zwischenspeichern
- Falls kein Ergebnis: Nachricht ungesichert senden

Diese Regel sollte in der Liste der Standardrichtlinien an 7. (letzter) Stelle aufgeführt sein.

Durch die opportunistische Verschlüsselung werden Nachrichten, für die ein verifizierter Schlüssel gefunden wird, signiert und verschlüsselt gesendet. Nachrichten, für die kein verifizierter Schlüssel gefunden wird, werden unverschlüsselt (als Klartext) gesendet. Auf diese Weise wird sichergestellt, dass Ihre Nachrichten gesendet werden, auch wenn einige als Klartext gesendet werden.

Diese Richtlinie sollte als letzter Eintrag in der Liste der Sicherheitsrichtlinien aufgeführt sein, da die Bedingungen der Richtlinie auf alle gesendeten Nachrichten zutreffen. Falls diese Richtlinie über einer anderen Richtlinie in der Liste angeordnet wird, erreicht PGP Desktop diese andere Richtlinie nie, sodass die Richtlinie nutzlos ist.

Standardrichtlinie „Verschlüsselung erzwingen: [PGP] Vertraulich“

„Verschlüsselung erzwingen: [PGP] Vertraulich“ ist eine der Standardsicherheitsrichtlinien, die von PGP Desktop automatisch für einen Dienst erstellt werden. Es gibt folgende Einstellungen für diese Standardrichtlinie:

- Falls: beliebige
- Bedingungen: Nachrichtenbetreff / enthält / [PGP] Nachrichtenvertraulichkeit / ist / vertraulich
- Aktionen: Signieren / Verschlüsseln an / verifizierten Schlüssel des Empfängers
- Bevorzugte Verschlüsselung: Automatisch
- Schlüssel nicht gefunden: keys.domain durchsuchen und / Alle Keyserver / Gefundene Schlüssel zwischenspeichern

Falls kein Ergebnis: Nachricht blockieren Diese Regel sollte in der Richtlinienliste an erster Stelle aufgeführt sein. Verschlüsselung erzwingen: [PGP] Vertraulich“ bewirkt, dass Nachrichten, die in der Betreffzeile den Text „[PGP]“ enthalten oder im E-Mail-Client als vertraulich gekennzeichnet sind, an einen verifizierten Schlüssel verschlüsselt werden müssen, um gesendet zu werden. Falls kein verifizierter Schlüssel gefunden werden kann, wird die Nachricht *nicht* gesendet.

Standardrichtlinie „Adressenlisten-Sendevorgänge“

„Adressenlisten-Sendevorgänge“ ist eine der Standardsicherheitsrichtlinien, die von PGP Desktop automatisch für einen Dienst erstellt werden.

Es gibt folgende Einstellungen für diese Standardrichtlinie:

- Falls: beliebige
- Bedingungen: Empfänger / stimmt mit Muster überein / .*-users@.*, .*-bugs@.*, .*-docs@.*, .*-help@.*, .*-news@.*, .*-digest@.*, .*-list@.*, .*-devel@.*, .*-announce@.*
- Aktionen: Signieren

Bevorzugte Verschlüsselung: PGP-partitioniert Diese Regel sollte in der Richtlinienliste an 6. Stelle aufgeführt sein.

Standardrichtlinie „Adressenlisten-Administratoranforderungen“

„Adressenlisten-Administratoranforderungen“ ist eine der Standardsicherheitsrichtlinien, die von PGP Desktop automatisch für einen Dienst erstellt werden.

Es gibt folgende Einstellungen für diese Standardrichtlinie:

- Falls: beliebige
- Bedingungen: Empfänger / stimmt mit Muster überein / .*-subscribe@.*, .*-unsubscribe@.*, .*-report@.*, .*-request@.*, .*-bounce@.*
- Aktionen: Klartext senden

Diese Regel sollte in der Richtlinienliste an 5. Stelle aufgeführt sein.

Beispiel für eine Richtlinie zur Erzwingung der Verschlüsselung an <Domäne>

Wenn Sie die Richtlinie „Opportunistische Verschlüsselung“ mit den Standardeinstellungen verwenden und die Richtlinie am Ende der Liste aufgeführt ist, werden Nachrichten, für die kein verifizierter Schlüssel gefunden wird, als Klartext übermittelt. Auf diese Weise wird sichergestellt, dass alle Nachrichten gesendet werden. Es bedeutet jedoch auch, dass einige Nachrichten möglicherweise unverschlüsselt gesendet werden.

Falls es bestimmte Domänen gibt, für die das Senden als Klartext nicht in Frage kommt, können Sie eine Sicherheitsrichtlinie erstellen, derzufolge eine Nachricht verschlüsselt und/oder signiert werden muss oder andernfalls *nicht* gesendet wird. Wenn Sie diese Richtlinie erstellen, achten Sie darauf, sie in der Liste über der Richtlinie „Opportunistische Verschlüsselung“ anzuordnen.

- Falls: beliebige
- Bedingungen: Empfängerdomäne / ist / beispiel.com

- Aktionen: Verschlüsseln an / verifizierten Schlüssel des Empfängers
- Bevorzugte Verschlüsselung: Automatisch
- Schlüssel nicht gefunden: keys.domain durchsuchen und / Alle Keyserver / Gefundene Schlüssel zwischenspeichern
- Falls kein Ergebnis: Nachricht blockieren

Diese Sicherheitsrichtlinie entspricht zum Teil der Richtlinie „Verschlüsselung erzwingen: [PGP] Vertraulich“, da sie vorsieht, dass eine Nachricht nur verschlüsselt gesendet werden kann. Das Auswahlkriterium ist jedoch nicht, ob die Nachricht als vertraulich gekennzeichnet ist, sondern ob die E-Mail-Domäne des Empfängers „beispiel.com“ lautet. Durch die Verwendung dieser Richtlinie wird sichergestellt, dass alle Nachrichten an „beispiel.com“ mit einem verifizierten Schlüssel verschlüsselt sind oder andernfalls nicht gesendet werden.

Beispiel für eine Richtlinie zum Signieren und Senden als Klartext an eine bestimmte Domäne

Falls Sie regelmäßig E-Mail-Nachrichten an eine Domäne senden, für die Sie alle Nachrichten zwar signieren, jedoch nicht verschlüsseln möchten, sollten Sie eine Richtlinie für die Domäne erstellen.

- Falls: beliebige
- Bedingungen: Empfängerdomäne / ist / beispiel.com
- Aktionen: Signieren
- Bevorzugte Verschlüsselung: Automatisch

Mit der Sicherheitsrichtlinienliste arbeiten

Es stehen verschiedene Möglichkeiten für die Sicherheitsrichtlinien in der Sicherheitsrichtlinienliste zur Verfügung. Beispielsweise können Sie eine Richtlinie bearbeiten, eine neue Richtlinie hinzufügen (siehe *Neue Sicherheitsrichtlinien erstellen* (auf Seite 112)) eine Richtlinie löschen oder die Reihenfolge der Richtlinien in der Liste ändern.

Sicherheitsrichtlinien bearbeiten

So bearbeiten Sie eine bestehende Sicherheitsrichtlinie

1 Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld „PGP Messaging“. Der PGP Messaging-Bildschirm wird angezeigt.

2 Klicken Sie auf den Namen des Dienstes mit der Sicherheitsrichtlinie, die Sie bearbeiten möchten. Die Eigenschaften des ausgewählten Dienstes werden angezeigt.

3 Wählen Sie die Sicherheitsrichtlinie aus, die Sie bearbeiten möchten, und klicken Sie auf **Richtlinie anzeigen**. Das Dialogfeld „Nachrichtenrichtlinie“ wird mit den Einstellungen für die angegebene Richtlinie geöffnet.

   Die Standardrichtlinien können angezeigt, geändert und deaktiviert, jedoch nicht gelöscht werden.

4 Nehmen Sie die gewünschten Änderungen an der Richtlinie vor. Informationen zu den Feldern im Dialogfeld „Nachrichtenrichtlinie“ finden Sie unter *Neue Sicherheitsrichtlinien erstellen* (auf Seite 112).

5 Nachdem Sie die gewünschten Änderungen vorgenommen haben, klicken Sie auf **OK**, um das Dialogfeld „Nachrichtenrichtlinie“ zu schließen. Die angegebene Sicherheitsrichtlinie wird geändert.

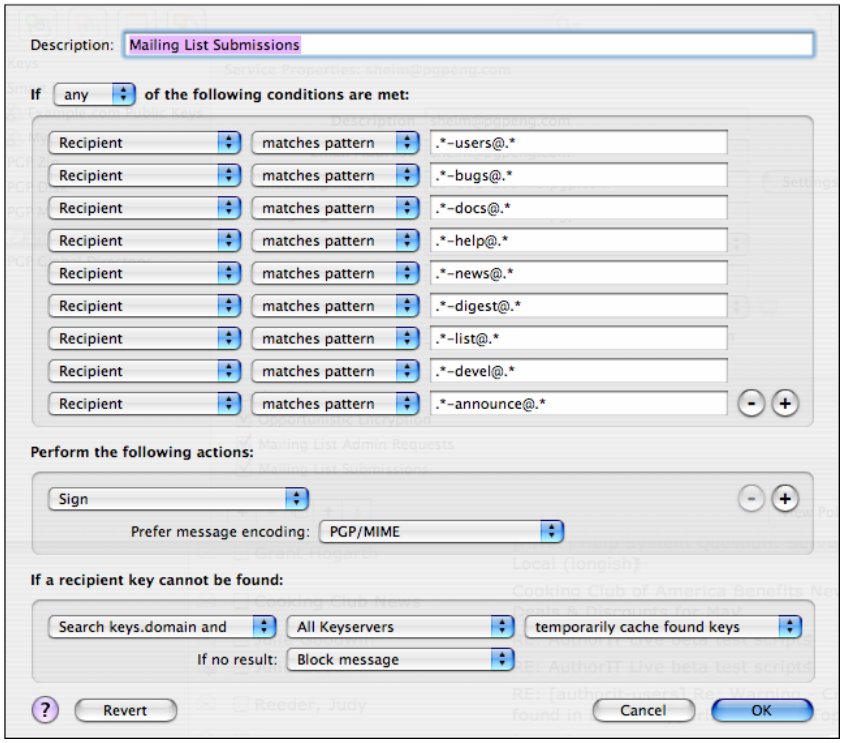
Adressenlisten-Richtlinien bearbeiten

▸ **So bearbeiten Sie eine standardmäßige Adressenlisten-Richtlinie**

1 Öffnen Sie PGP Desktop und klicken Sie auf das Bedienfeld „PGP Messaging“. Der PGP Messaging-Bildschirm wird angezeigt.

2 Klicken Sie auf den Namen des Dienstes mit der Sicherheitsrichtlinie, die Sie bearbeiten möchten. Die Eigenschaften des ausgewählten Dienstes werden angezeigt.

3 Wählen Sie die Adressenlisten-Richtlinie aus, die Sie bearbeiten möchten, und klicken Sie auf **Richtlinie anzeigen**. Das Dialogfeld „Nachrichtenrichtlinie“ wird mit den Einstellungen für die angegebene Richtlinie geöffnet.


Description: Mailing List Submissions
If any of the following conditions are met:
Recipient matches pattern .*-users@.*
Recipient matches pattern .*-bugs@.*
Recipient matches pattern .*-docs@.*
Recipient matches pattern .*-help@.*
Recipient matches pattern .*-news@.*
Recipient matches pattern .*-digest@.*
Recipient matches pattern .*-list@.*
Recipient matches pattern .*-devel@.*
Recipient matches pattern .*-announce@.*
Perform the following actions:
Sign
Prefer message encoding: PGP/MIME
If a recipient key cannot be found:
Search keys.domain and All Keyservers temporarily cache found keys
If no result: Block message
Revert
Cancel
OK

Die Standardrichtlinien können angezeigt, geändert und deaktiviert, jedoch nicht gelöscht werden.

4 Nehmen Sie die gewünschten Änderungen an der Richtlinie vor. Wählen Sie im ersten Feld Folgendes aus:

- **Falls beliebige**: Die Richtlinie wird angewendet, wenn eine der Bedingungen erfüllt ist.
- **Falls alle**: Die Richtlinie wird nur angewendet, wenn alle Bedingungen erfüllt sind.
- **Falls keine**: Die Richtlinie wird nur angewendet, wenn keine der Bedingungen erfüllt ist.

5 Wählen Sie im ersten Bedingungsfeld Folgendes aus:

- **Empfänger**: Die Richtlinie wird nur auf Nachrichten an den angegebenen Empfänger angewendet.
- **Empfängerdomäne**: Die Richtlinie wird nur auf E-Mail-Nachrichten in der angegebenen Empfängerdomäne angewendet.
- **Absender: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Absenderadresse angewendet.**

- **Nachricht: Die Richtlinie wird nur auf Nachrichten mit dem angegebenen Signierungs- und/oder Verschlüsselungsstatus angewendet.**
- **Nachrichtenbetreff**: Die Richtlinie wird nur auf Nachrichten mit dem angegebenen Nachrichtenbetreff angewendet.
- **Nachrichtenkopf**: Die Richtlinie wird nur auf Nachrichten angewendet, bei denen die angegebene Kopfzeile die festgelegten Kriterien erfüllt. Beachten Sie, dass die im nächsten Abschnitt beschriebenen Bedingungen (ist, ist nicht, enthält usw.) für den Text gelten, der in das Textfeld eingegeben wird, das nach Auswahl von **Nachrichtenkopf** angezeigt wird.

Hinweis: Die Suche nach Nachrichtenköpfen in Lotus Notes- und MAPI-E-Mail-Systemen ist nicht implementiert, da Nachrichten in diesen Systemen keinen Nachrichtenkopf aufweisen.

- **Nachrichtentext**: Die Richtlinie wird nur auf Nachrichten mit dem angegebenen Nachrichtentext angewendet.
- **Nachrichtengröße: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Größe (in Byte) angewendet.**
- **Nachrichtenpriorität**: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Nachrichtenpriorität angewendet.
- **Nachrichtenvertraulichkeit**: Die Richtlinie wird nur auf Nachrichten mit der angegebenen Nachrichtenvertraulichkeit angewendet.

6 Wählen Sie im zweiten Bedingungsfeld Folgendes aus:

- **ist**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *übereinstimmt*.
- **ist nicht**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *nicht übereinstimmt*.
- **enthält**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld den Text im Textfeld *enthält*.
- **enthält nicht**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld den Text im Textfeld *nicht enthält*.
- **beginnt mit**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *beginnt*.
- **endet mit**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Text im Textfeld *endet*.
- **stimmt mit Muster überein**: Die Bedingung ist erfüllt, wenn der Text im ersten Bedingungsfeld mit dem Textmuster im Textfeld *übereinstimmt*.

7 Geben Sie im dritten Bedingungsfeld in das Textfeld den Text für die Übereinstimmungskriterien ein.

8 Wählen Sie im Bereich „Für die Nachricht folgende Aktionen ausführen" im ersten Aktionsfeld Folgendes aus:

- **Klartext senden**: Gibt an, dass die Nachricht als Klartext gesendet werden soll, d. h. weder signiert noch verschlüsselt.
- **Signieren**: Gibt an, dass die Nachricht signiert werden soll.
- **Verschlüsseln an**: Gibt an, dass die Nachricht verschlüsselt werden soll.

9 Wählen Sie im zweiten Aktionsfeld Folgendes aus:

- **verifizierten Schlüssel des Empfängers**: Gewährleistet, dass die Nachricht nur an einen verifizierten Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann.
- **nicht verifizierten Schlüssel des Empfängers**: Ermöglicht, dass die Nachricht an einen nicht verifizierten Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann.

verifizierten End-to-End-Schlüssel des Empfängers: Gewährleistet, dass die Nachricht nur an einen verifizierten End-to-End-Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann. Ein End-to-End-Schlüssel befindet sich im alleinigen Besitz des jeweiligen Empfängers. In einer von einem PGP Universal Server verwalteten Umgebung ist dies ein CKM-Schlüssel (Client Key Mode). Im Gegensatz dazu befindet sich ein SKM-Schlüssel (Server Key Mode) im Besitz des PGP Universal Servers.

Ob es sich um einen End-to-End-Schlüssel handelt, wird unter Windows im Dialogfeld „Schlüsseleigenschaften" und unter Mac OS X im Dialogfeld „Schlüssel-Info" im Feld **Gruppe** angezeigt. **Nein** bedeutet, dass es ein End-to-End-Schlüssel (d. h. nicht Teil einer Gruppe) *ist*, und **Ja** bedeutet, dass es sich *nicht* um einen End-to-End-Schlüssel handelt.

- **nicht verifizierten End-to-End-Schlüssel des Empfängers**: Ermöglicht, dass die Nachricht an einen nicht verifizierten End-to-End-Schlüssel des beabsichtigten Empfängers verschlüsselt werden kann.
- **eine Liste von Schlüsseln**: Gibt an, dass die Nachricht nur an Schlüssel in der Liste verschlüsselt werden kann.

10 Wählen Sie im Feld für die bevorzugte Nachrichtenverschlüsselung Folgendes aus:

- **Automatisch**: Das Nachrichtenverschlüsselungsformat wird von PGP Desktop ausgewählt. Dies ist die empfohlene Einstellung. Wählen Sie nur dann eine andere Option aus, wenn Sie genau wissen, warum Sie eines der anderen Nachrichtenverschlüsselungsformate benötigen.
- **PGP-partitioniert**: Legt „PGP-partitioniert" als bevorzugtes Nachrichtenverschlüsselungsformat fest. Dieses Format gewährleistet die größte Rückwärtskompatibilität mit älteren PGP- und OpenPGP-Produkten.

- **PGP/MIME**: Legt „PGP/MIME“ als bevorzugtes Nachrichtenverschlüsselungsformat fest. Mit PGP/MIME kann die gesamte Nachricht, einschließlich Anlagen, in einem Durchgang verschlüsselt und signiert werden, was schneller ist und zu einer besseren Wiedergabe der gesamten Nachricht führt.
- **S/MIME**: Legt „S/MIME“ als bevorzugtes Nachrichtenverschlüsselungsformat fest. Wählen Sie „S/MIME“ aus, wenn Sie dieses Format verwenden müssen, obwohl der Benutzer über einen PGP-Schlüssel verfügt.

11 Wählen Sie im Bereich **Falls der Schlüssel des Empfängers nicht verfügbar ist** im ersten Feld **Folgendes aus:**

- **keys.domain durchsuchen und**: Gibt an, dass die Suche sowohl in keys.domain als auch auf einem anderen, von Ihnen angegebenen Server durchgeführt wird.
- **Suchen**: Ermöglicht die Suche nach einem entsprechenden Schlüssel, wenn am lokalen Schlüsselbund kein Schlüssel gefunden wird.
- **Nachricht als Klartext signieren**: Gibt an, dass die Nachricht als Klartext gesendet werden soll, jedoch signiert wird.
- **Nachricht ungesichert senden**: Gibt an, dass die Nachricht als Klartext gesendet werden soll.
- **Nachricht blockieren**: Gibt an, dass die Nachricht nicht gesendet werden soll, wenn kein entsprechender Schlüssel gefunden wird.

12 Wählen Sie im zweiten Feld Folgendes aus:

- **Alle Keyserver**: Gibt an, dass alle Keyserver, einschließlich des PGP Global Directory, nach einem entsprechenden Schlüssel durchsucht werden sollen.
- **PGP Global Directory bzw. keyserver.pgp.com**: Gibt an, dass nur das PGP Global Directory durchsucht wird.
- **[konfigurierte Keyserver]**: Gibt an, dass nur der Keyserver durchsucht wird, den Sie aus der Liste der aktuell konfigurierten Keyserver auswählen. Beachten Sie, dass andere Keyserver als das PGP Global Directory möglicherweise nicht verifizierte Schlüssel bereitstellen. Diese können nicht verwendet werden, wenn laut Richtlinie verifizierte Schlüssel erforderlich sind. Sofern Sie nicht genau wissen, warum ein bestimmter anderer Keyserver durchsucht werden soll, und Sie darauf vorbereitet sind, diese Schlüssel bei Bedarf manuell zum Verifizieren zu suchen, sollten Sie nur das PGP Global Directory durchsuchen. Diese Option ist nur unter Windows verfügbar.
- **Keyserver-Liste bearbeiten**: Ermöglicht Ihnen das Hinzufügen von Keyservern zur Liste der aktuell konfigurierten Keyserver. Diese Option ist nur unter Windows verfügbar.

13 Wählen Sie im letzten Feld Folgendes aus:

- **Gefundene Schlüssel zwischenspeichern**: Gibt an, dass ein gefundener Schlüssel zwischengespeichert werden soll. Die Schlüssel in diesem Zwischenspeicher werden automatisch zum Verifizieren signierter Nachrichten verwendet. Wenn Sie verifiziert wurden, werden Sie für die Verschlüsselung genutzt.
- **Zum Speichern gefundener Schlüssel auffordern**: Gibt an, dass PGP Desktop anfragen soll, ob Sie einen bestimmten gefundenen Schlüssel am lokalen Schlüsselbund speichern möchten.
- **Gefundene Schlüssel speichern**: Gibt an, dass gefundene Schlüssel automatisch am lokalen Schlüsselbund gespeichert werden sollen.

14 Wählen Sie in der Liste „Falls kein Ergebnis“ Folgendes aus:

- **Nachricht als Klartext signieren**: Ermöglicht, dass Nachrichten, für die kein Verschlüsselungsschlüssel gefunden wird, signiert und als Klartext gesendet werden.
- **Nachricht ungesichert senden**: Die Nachricht wird nicht verschlüsselt.
- **Nachricht blockieren**: Verhindert, dass Nachrichten gesendet werden, für die kein Verschlüsselungsschlüssel gefunden wurde.

15 Nachdem Sie die gewünschten Änderungen vorgenommen haben, klicken Sie auf **OK**, um das Dialogfeld „Nachrichtenrichtlinie“ zu schließen. Die angegebene Sicherheitsrichtlinie wird geändert.

Sicherheitsrichtlinien löschen

▸ **So löschen Sie eine bestehende Sicherheitsrichtlinie**

1 Klicken Sie auf den Namen des Dienstes mit der Sicherheitsrichtlinie, die Sie löschen möchten. Die Eigenschaften des ausgewählten Dienstes werden angezeigt.

2 Deaktivieren Sie das Kontrollkästchen neben der Richtlinie, die Sie löschen möchten.

3 Vergewissern Sie sich, dass die Richtlinie weiterhin ausgewählt ist. Klicken Sie unten im Bereich **Sicherheitsrichtlinien** auf **[-]. Ein Bestätigungsdialogfeld wird angezeigt.**

4 Klicken Sie auf **Entfernen**, um die Richtlinie zu löschen. Die ausgewählte Sicherheitsrichtlinie wird aus der Liste entfernt.

Reihenfolge der Richtlinien in der Liste ändern

▸ **So ändern Sie die Reihenfolge der Richtlinien in der Sicherheitsrichtlinienliste**

1. Klicken Sie im Bedienfeld „PGP Messaging“ auf den Namen des Dienstes mit der Sicherheitsrichtlinie, deren Reihenfolge Sie ändern möchten. Die Eigenschaften des ausgewählten Dienstes werden angezeigt.
2. Klicken Sie in der Liste **Sicherheitsrichtlinien** auf den Namen der Richtlinie, deren Reihenfolge in der Liste Sie ändern möchten. Die angegebene Richtlinie wird hervorgehoben.
3. Klicken Sie unten im Fenster „Sicherheitsrichtlinien“ auf den Pfeil nach oben oder den Pfeil nach unten, bis sich die Richtlinie an der gewünschten Stelle in der Liste befindet.

Hinweis: Achten Sie darauf, dass die Richtlinie **Opportunistische Verschlüsselung** am Ende der Liste aufgeführt ist. Alle danach folgenden Richtlinien werden nicht implementiert.

PGP Desktop und SSL

Wenn Sie PGP Desktop verwenden, zielt die PGP Corporation darauf ab, Ihre Daten nach Möglichkeit automatisch zu sichern. Dazu gehört der Schutz der Daten bei der Übertragung zwischen dem E-Mail-Client und dem E-Mail-Server.

Tipp: SSL ist die Abkürzung für Secure Sockets Layer, ein kryptografisches Protokoll zum Sichern der Kommunikation zwischen zwei Geräten. In diesem Fall sichert es die Kommunikation zwischen dem E-Mail-Client bzw. PGP Desktop und dem E-Mail-Server.

Abhängig von den jeweiligen Bedingungen schützt PGP Desktop die Daten auf dem Übertragungsweg zum und vom E-Mail-Server auf verschiedene Weise. Die folgenden Informationen gelten nur, wenn Sie im Dialogfeld „Servereinstellungen“ für die SSL/TLS-Einstellung die Option **Automatisch** (Standardeinstellung) ausgewählt haben:

- **Wenn die Verbindung nicht durch SSL geschützt ist:** Wenn die Verbindung zwischen dem E-Mail-Client und dem E-Mail-Server nicht durch SSL geschützt ist, versucht PGP Desktop automatisch, für diese Verbindung SSL zu verwenden (d. h. die Anwendung kommuniziert mit dem E-Mail-Server und verwendet SSL, wenn dies vom E-Mail-Server unterstützt wird).

Wenn der E-Mail-Server SSL nicht unterstützt, werden die Nachrichten, die von PGP Desktop während der Sitzung gesendet und empfangen werden, über eine ungeschützte Verbindung übertragen. PGP Desktop versucht grundsätzlich, eine SSL-Verbindung aufzubauen, unabhängig davon, ob PGP Desktop die Nachrichten verschlüsselt oder entschlüsselt. Nachrichten, die von PGP Desktop verschlüsselt wurden, können über eine durch SSL geschützte Verbindung oder über eine ungeschützte Verbindung gesendet und empfangen werden.

Hinweis: Bei einer ungeschützten Verbindung zum E-Mail-Server versucht PGP Desktop grundsätzlich, den SSL-Schutz zu aktivieren, **da bei einer durch SSL geschützten Verbindung nicht nur alle mit der PGP-Anwendung verschlüsselten Nachrichten zwischen E-Mail-Server und E-Mail-Client geschützt werden, sondern auch die Authentifizierungspassphrase des E-Mail-Servers, wenn sie an den E-Mail-Server gesendet wird.**

- **Wenn die Verbindung durch SSL geschützt ist:** Wenn im E-Mail-Client der SSL-Schutz für die Verbindung zum E-Mail-Server aktiviert wurde und PGP Desktop Ihre Nachrichten verschlüsseln oder entschlüsseln soll, müssen Sie den Schutz deaktivieren. PGP Desktop kann die Nachrichten nicht verarbeiten, wenn sie bereits mit SSL verschlüsselt sind.

  Wenn der SSL-Schutz im E-Mail-Client deaktiviert wurde, bedeutet dies nicht, dass Nachrichten, die nicht mit der PGP-Anwendung verschlüsselt wurden, bei der Übertragung vom und zum E-Mail-Server ungeschützt sind. Wie bei jeder Verbindung, die nicht durch SSL geschützt ist, versucht PGP Desktop automatisch, für diese Verbindung den SSL-Schutz zu aktivieren, wenn dieser vom E-Mail-Server unterstützt wird (falls Sie im Dialogfeld „Servereinstellungen“ für die SSL/TLS-Einstellung die Option **Automatisch** ausgewählt haben). Wenn der E-Mail-Server keine SSL-Verbindungen unterstützt, sendet PGP Desktop die Nachrichten während der Sitzung über eine ungeschützte Verbindung.

  Ihre Nachrichten werden nur dann als Klartext an den E-Mail-Server gesendet, wenn die Nachrichten nicht mit der PGP-Anwendung verschlüsselt sind und die Verbindung zum E-Mail-Server nicht durch SSL geschützt werden kann oder wenn Sie für die SSL/TLS-Einstellung die Option **Nicht versuchen** ausgewählt haben.

- **Wenn Nachrichten nicht als Klartext gesendet werden dürfen:** In einigen Sicherheitsrichtlinien ist festgelegt, dass nur geschützte und keine ungeschützten Nachrichten gesendet werden dürfen. Bei Bedarf können Sie PGP Desktop so konfigurieren, dass derartige Sicherheitsrichtlinien unterstützt werden.

  Wählen Sie den entsprechenden PGP Messaging-Dienst aus und öffnen Sie das Dialogfeld „Servereinstellungen“ (klicken Sie auf den Namen des Servers, der derzeit für den Dienst in den Kontoeigenschaften im Feld für den Server ausgewählt ist). Wählen Sie in der Liste „SSL/TLS“ eine *andere* Option als **Automatisch** aus.

Wenn diese Option aktiviert ist, wird das Senden und Empfangen von Nachrichten zwischen dem E-Mail-Server und PGP Desktop nur über eine durch SSL geschützte Verbindung abgewickelt. Falls keine durch SSL geschützte Verbindung hergestellt werden kann, kommuniziert PGP Desktop nicht mit dem Server.

Hinweis: Diese Option darf nur aktiviert werden, wenn Sie sicher sind, dass der E-Mail-Server das SSL-Protokoll unterstützt. Auf diese Weise wird sichergestellt, dass PGP Desktop keine Nachrichten über ungeschützte Verbindungen sendet oder empfängt, falls beispielsweise ein Problem bei der Aushandlung des SSL-Protokolls für die Verbindung auftritt. Wenn Sie diese Option aktivieren und der E-Mail-Server SSL nicht unterstützt, sendet oder empfängt PGP Desktop keine Nachrichten.

- **Wenn SSL im E-Mail-Client aktiviert sein soll:** Damit Sie PGP Desktop verwenden können, wenn SSL im E-Mail-Client aktiviert ist, müssen Sie die Option **Bei SSL/TLS-Verbindungsversuch durch E-Mail-Client warnen** für den Mailserver für eingehende Nachrichten, für den Postausgangsserver oder für beide Server deaktivieren. Wenn diese Option für eine Verbindung zu einem E-Mail-Server deaktiviert ist, ignoriert PGP Desktop den ein- und ausgehenden E-Mail-Verkehr über diese Verbindung, wenn die Verbindung durch SSL geschützt ist.

  PGP Desktop überwacht die Verbindungen zu und von diesem Server und ignoriert den E-Mail-Verkehr, der über Verbindungen gesendet oder empfangen wird, die durch SSL geschützt sind. Falls PGP Desktop jedoch eine Verbindung erkennt, die nicht durch SSL geschützt ist, wird der Verkehr wie alle anderen ungeschützten Verbindungen gehandhabt. Die Anwendung versucht, für diese Verbindung den SSL-Schutz zu aktivieren (wenn der Modus „Automatisch“ ausgewählt ist) und entsprechende Richtlinien auf die Nachrichten anzuwenden.

Schlüsselmodi

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, arbeitet PGP Desktop in einem Schlüsselmodus.

Hinweis: Die Informationen in diesem Abschnitt gelten *nur* für Benutzer, die PGP Desktop in einer von einem PGP Universal Server geschützten E-Mail-Domäne einsetzen.

Folgende Schlüsselmodi sind verfügbar:

- **Server Key Mode (SKM):** Schlüssel werden auf dem PGP Universal Server erstellt und von diesem verwaltet. Sie werden ausschließlich bei Bedarf für den Computer freigegeben, auf dem Sie PGP Desktop ausführen. Ihr privater Schlüssel wird nur auf dem PGP Universal Server gespeichert, der auch die gesamte diesbezügliche Verwaltung übernimmt. Da der PGP Universal-Administrator vollständigen Zugriff auf Ihren privaten Schlüssel hat, kann er auf alle Nachrichten zugreifen, die Sie verschlüsseln. Dieser Schlüsselmodus ist *nicht* mit Smartcards kompatibel (Smartcards können nur unter Windows verwendet werden).

  Ab PGP Desktop Version 10.0 können SKM-Schlüssel, die zuvor nur für Messaging verwendet werden konnten, für alle anderen PGP Desktop-Verschlüsselungsvorgänge genutzt werden. Dies umfasst das Verschlüsseln von Laufwerken und Dateien und das Entschlüsseln von MAPI-E-Mail-Nachrichten im Offlinemodus.

  Wenn Sie einen SKM-Schlüssel verwenden, entfällt generell die Notwendigkeit, eine Passphrase zur Authentifizierung einzugeben. SKM-Schlüsselpassphrasen werden von PGP Desktop auf Zufallsbasis erzeugt und verschlüsselt gespeichert. Wenn PGP Desktop eine Passphrase erfordert, ruft PGP Desktop die verschlüsselte Passphrase vom System ab, ohne dass eine Aktion Ihrerseits erforderlich ist.

- **Client-Schlüsselmodus (CKM):** Schlüssel werden auf dem Computer erstellt und verwaltet, auf dem Sie PGP Desktop ausführen. Private Schlüssel werden nicht für den PGP Universal Server freigegeben. Auch alle kryptografischen Operationen (Verschlüsseln, Entschlüsseln, Signieren, Verifizieren) werden auf dem Computer durchgeführt, auf dem Sie PGP Desktop ausführen. Unter Windows ist dieser Schlüsselmodus mit Smartcards kompatibel.

- **Guarded Key Mode (GKM):** Dieser Modus ähnelt CKM, jedoch wird eine *verschlüsselte* Kopie des privaten Schlüssels auf dem PGP Universal Server gespeichert, auf den Sie über einen anderen Computer zugreifen können. Da der Schlüssel verschlüsselt ist, kann der PGP Universal-Administrator nicht darauf zugreifen und der Zugriff ist ausschließlich Ihnen vorbehalten. Dieser Schlüsselmodus ist mit Smartcards kompatibel (nur unter Windows), sofern der Schlüssel nicht direkt auf der Smartcard erstellt wird (d. h. der Schlüssel muss auf die Smartcard kopiert werden).

- **Server Client Key Mode (SCKM):** Dieser Modus ist ebenfalls mit CKM vergleichbar, jedoch wird eine Kopie des privaten *Verschlüsselungsschlüssel* auf dem PGP Universal Server gespeichert. Private *Signaturschlüssel* befinden sich grundsätzlich nur auf dem Computer, auf dem Sie PGP Desktop ausführen. Dieser Schlüsselmodus dient der Einhaltung von Gesetzen und Unternehmensrichtlinien, die verlangen, dass der Benutzer stets die Kontrolle über den privaten Signaturschlüssel behält, während der private Verschlüsselungsschlüssel gespeichert wird und in Notfällen zugänglich ist. Dieser Schlüsselmodus ist mit Smartcards kompatibel (nur unter Windows), sofern der Schlüssel nicht direkt auf der Smartcard erstellt wird. Für SCKM ist ein Schlüssel mit einem separaten Signatur-Unterschlüssel erforderlich, der mit PGP Desktop 9.5 oder höher für einen neuen Schlüssel erstellt oder mit PGP Desktop 9.5 oder höher einem älteren Schlüssel hinzugefügt werden kann.

Abhängig von der Konfiguration Ihrer Version von PGP Desktop durch den PGP-Administrator können Sie den Schlüsselmodus möglicherweise nicht auswählen. Von der Konfiguration hängt auch ab, ob Sie den Schlüsselmodus ändern können.

Wenden Sie sich an den PGP-Administrator, wenn Sie weitere Fragen zum Schlüsselmodus haben.

Schlüsselmodus ermitteln

Beachten Sie, dass nur PGP Desktop-Benutzer in einer mit PGP Universal geschützten Umgebung über einen Schlüsselmodus verfügen, nicht jedoch Benutzer eigenständiger Versionen von PGP Desktop.

So ermitteln Sie Ihren Schlüsselmodus

- Öffnen Sie PGP Desktop und wählen Sie den PGP Messaging-Dienst aus, dessen Schlüsselmodus Sie ermitteln möchten. Die Kontoeigenschaften und Sicherheitsrichtlinien für den ausgewählten Dienst werden angezeigt.

  Im Feld **Universal-Server** ist der Schlüsselmodus für den ausgewählten Dienst in Klammern hinter dem Namen des PGP Universal Servers angegeben (z. B. **keys.beispiel.com (GKM)**). Der Schlüsselmodus für den ausgewählten Dienst ist in diesem Beispiel also Guarded Key Mode (GKM) und der zugehörige PGP Universal Server ist keys.beispiel.com.

Schlüsselmodus ändern

Abhängig von der Konfiguration Ihrer Version von PGP Desktop durch den PGP-Administrator können Sie den Schlüsselmodus möglicherweise nicht ändern.

So ändern Sie den Schlüsselmodus

1. Öffnen Sie PGP Desktop und wählen Sie den PGP Messaging-Dienst aus, dessen Schlüsselmodus Sie ändern möchten. Die Kontoeigenschaften und Sicherheitsrichtlinien für den ausgewählten Dienst werden angezeigt.
2. Klicken Sie auf **Schlüsselmodus**. Der Bildschirm für den PGP Universal-Schlüsselmodus wird geöffnet und enthält Informationen zum aktuellen Schlüsselverwaltungsmodus.
3. Klicken Sie auf **Schlüssel zurücksetzen** und klicken Sie in der daraufhin angezeigten Bestätigungsmeldung auf **Ja**. Der Einrichtungsassistent für PGP-Schlüssel wird geöffnet.
4. Lesen Sie den angezeigten Text und klicken Sie auf **Weiter**. Der Bildschirm „Schlüsselverwaltung auswählen“ wird angezeigt.
5. Wählen Sie den gewünschten Schlüsselmodus aus. Abhängig von der Konfiguration Ihrer Kopie von PGP Desktop durch den PGP Universal-Administrator stehen Ihnen einige Schlüsselmodi möglicherweise nicht zur Verfügung.
6. Klicken Sie auf **Weiter**. Der Bildschirm „Schlüsselquelle auswählen“ wird angezeigt.
7. Wählen Sie eine der folgenden Optionen aus:
   - **Neuer Schlüssel**: Sie werden aufgefordert, einen neuen PGP-Schlüssel zu erstellen, der zum Schutz des Messaging-Verkehrs verwendet wird.
   - **PGP Desktop-Schlüssel**: Sie werden aufgefordert, einen vorhandenen PGP-Schlüssel anzugeben, der zum Schutz des Messaging-Verkehrs verwendet wird.
   - **Schlüssel importieren**: Sie werden aufgefordert, einen PGP-Schlüssel zu importieren, der zum Schutz des Messaging-Verkehrs verwendet wird.
8. Wählen Sie die gewünschte Option aus und klicken Sie auf **Weiter**.
9. Wenn Sie **Neuer Schlüssel** ausgewählt haben, führen Sie folgende Schritte aus:
   - Geben Sie eine Passphrase für den Schlüssel ein und klicken Sie auf **Weiter**.
   - Wenn der Schlüssel erstellt wurde, klicken Sie auf **Weiter**.
   - Klicken Sie auf **Beenden**.
10. Wenn Sie **PGP Desktop-Schlüssel** ausgewählt haben, führen Sie folgende Schritte aus:
    - Wählen Sie den gewünschten Schlüssel auf dem lokalen Schlüsselbund aus und klicken Sie auf **Weiter**.
    - Klicken Sie auf **Beenden**.

11 Wenn Sie **Schlüssel importieren** ausgewählt haben, führen Sie folgende Schritte aus:

- Wechseln Sie zu der Datei mit dem PGP-Schlüssel, den Sie importieren möchten (Datei muss einen privaten Schlüssel enthalten). Klicken Sie dann auf **Weiter**.
- Klicken Sie auf **Beenden**.

PGP-Protokoll anzeigen

Im PGP-Protokoll werden die Aktionen angezeigt, die von PGP Desktop zum Schutz Ihrer Nachrichten ergriffen werden.

So zeigen Sie das PGP-Protokoll an

1 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf das PGP Desktop-Symbol in der Menüleiste und wählen Sie aus dem Menü die Option **Protokoll anzeigen** aus. Das PGP-Protokoll wird angezeigt.
- Öffnen Sie PGP Desktop und klicken Sie auf **Fenster > PGP-Protokoll**. Das PGP-Protokoll wird angezeigt.

2 Führen Sie folgende Schritte aus:

- Klicken Sie auf **Löschen**, um alle Einträge im PGP-Protokoll zu löschen. Wenn Sie aufgefordert werden, den Löschvorgang zu bestätigen, klicken Sie auf **Ja**.
- Klicken Sie auf **Finden, um nach Einträgen im PGP-Protokoll zu suchen. Geben Sie die Suchbegriffe ein und klicken Sie auf Weiter**.
- Klicken Sie auf den Pfeil für das Menü **Protokollierungsstufe, um auszuwählen, welche Protokolleinträge mindestens angezeigt werden sollen: Info** oder **Ausführlich**. Beachten Sie, dass die Option **Ausführlich** zu sehr großen Protokolldateien führen kann.

  Wenn Sie Protokolle anzeigen möchten, die mit der Option **Ausführlich** aufgezeichnet wurden, muss das Anzeigefenster für das PGP-Protokoll geöffnet bleiben. Wenn Sie das Fenster schließen, kehrt das System zur Standardprotokollierungsstufe **Info** zurück. Beachten Sie, dass die Option **Ausführlich** zu sehr großen Protokolldateien führen kann.
- Klicken Sie auf **Speichern**, um eine Kopie der Protokolleinträge zu speichern. Geben Sie den Dateinamen, den Speicherort und das Format (standardmäßig wird eine Textdatei erstellt) für die Protokolldatei an und klicken Sie auf **Speichern**.

3 Klicken Sie auf den roten Kreis oben links im Bildschirm, um das Fenster mit dem PGP-Protokoll zu schließen.

PGP-Skripte mit Entourage 2008 verwenden

So verwenden Sie PGP-Skripte in Entourage zum Verschlüsseln von E-Mail-Nachrichten

1 Erstellen Sie eine E-Mail-Nachricht.

2 Klicken Sie in der Entourage-Symbolleiste auf das Symbol für Skripte **und wählen Sie PGP** aus.

3 Wählen Sie die Option **Verschlüsseln** oder **Verschlüsseln und signieren** aus sowie den Schlüssel, der zum Signieren verwendet werden soll.

4 Der E-Mail-Text wird verschlüsselt und stattdessen wird Ciphertext angezeigt.

5 Sie können die E-Mail-Nachricht jetzt sicher senden.

So verwenden Sie die PGP-Skripte in Entourage zum Entschlüsseln von E-Mail-Nachrichten

1 Öffnen Sie die verschlüsselte E-Mail-Nachricht.

2 Klicken Sie im Menü auf die Option für Skripte **und wählen Sie PGP** aus.

3 Wählen Sie **Entschlüsseln und verifizieren** aus und geben Sie bei der Aufforderung die Passphrase ein. Die E-Mail-Nachricht wird entschlüsselt.

9 Instant Messaging-Sitzungen sichern

In diesem Abschnitt finden Sie Informationen zum Sichern von Instant Messaging-Sitzungen (IM) mit PGP Desktop. Informationen zu PGP-Optionen für IM-Sitzungen finden Sie unter *Messaging-Optionen* (siehe "*Messaging-Einstellungen*" auf Seite 223).

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat der PGP Universal Server-Administrator möglicherweise bestimmte Funktionen deaktiviert. Wenn eine Funktion deaktiviert wurde, wird das entsprechende Bedienelement auf der linken Seite nicht angezeigt und das Menü und andere Optionen für diese Funktion sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn der PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Informationen zur Instant Messaging-Kompatibilität von PGP Desktop 139
Informationen zu den für die Verschlüsselung verwendeten Schlüsseln141
IM-Sitzungen verschlüsseln..... 141

Informationen zur Instant Messaging-Kompatibilität von PGP Desktop

PGP Desktop verschlüsselt automatisch standardmäßige AOL- und iChat-IM-Sitzungen, Direktverbindungen und Dateiübertragungen, wenn folgende Bedingungen erfüllt sind:

- Auf dem System beider Teilnehmer, auf dem die IM-Anwendung verwendet wird, ist PGP Desktop 9.0 oder höher installiert und wird ausgeführt. Wenn Sie bestätigen möchten, dass Sie PGP Desktop 9.0 oder höher verwenden, klicken Sie auf das PGP-Symbol im Infobereich der Taskleiste und wählen Sie im Kontextmenü die Option **Info über PGP** aus. (Wählen Sie im Fenster von PGP Desktop die Option **Hilfe > Info über PGP** aus.)

- Beide Teilnehmer haben die Option **zum Verschlüsseln von Instant Messages aktiviert. Führen Sie dazu folgende Schritte aus:**
  - Wählen Sie unter Windows die Option **Extras > Optionen**, klicken Sie auf die Registerkarte „Messaging“ und aktivieren Sie das Kontrollkästchen **AOL Instant Messaging-Nachrichten (AIM) verschlüsseln**.
  - Wählen Sie unter Mac OS X die Option **PGP > Einstellungen** aus, klicken Sie auf das Symbol „Messaging“ und aktivieren Sie das Kontrollkästchen **AOL Instant Messaging-Nachrichten (AIM) verschlüsseln**.

  Tipp: Unter Windows können Sie schnell bestätigen, dass die Instant Messaging-Verschlüsselung aktiviert ist, indem Sie auf das PGP-Symbol im Infobereich der Taskleiste klicken. Im Kontextmenü sollte neben der Option **AIM-Proxy verwenden** ein Häkchen angezeigt werden.
- Beide Benutzer verwenden kompatible IM-Clients. Informationen zu kompatiblen IM-Clients finden Sie im folgenden Abschnitt.
- Die AIM-Adresse des Initiators der IM-Sitzung **ist** in der Buddy-Liste des Empfängers der Sitzung aufgeführt (andernfalls wird die Sitzung nicht verschlüsselt).

Die sichere IM-Funktion ist mit allen IM-Clients kompatibel, die das OSCAR-Protokoll für Instant Messaging von AOL unterstützen, z. B. AOL Instant Messenger, Trillian Pro, iChat und Gaim.

Für die Sitzungen für Dateiübertragung und Direktverbindung sind aktuelle Versionen dieser Clients erforderlich, damit sie von PGP Desktop verschlüsselt werden können. Darüber hinaus empfiehlt die PGP Corporation, beide Verbindungen (Direct IM/Direct Message und Dateiübertragung) so zu konfigurieren, dass der AOL-Proxy verwendet wird und der Buddy nicht direkt mit Ihrem Computer verbunden ist.

Hinweise:

Audio- und Videoverbindungen werden von PGP Desktop nicht verschlüsselt.

Die sichere IM-Funktion von PGP Desktop setzt zur Erhöhung der Sicherheit PFS (Perfect Forward Secrecy) ein. Alle zur Sicherung der IM-Sitzungen verwendeten Schlüssel werden zu Beginn der Verbindung erstellt und bei Trennung der Verbindung vernichtet. Für jede IM-Sitzung werden vollkommen neue Schlüsselsätze verwendet. Die Sicherheitsstufe von IM-Sitzungen wird dadurch zusätzlich erhöht.

Kompatibilität mit Instant Messaging-Clients

PGP Desktop ist bei der Verschlüsselung von AIM-Nachrichten, -Dateiübertragungen und -Direktverbindungen mit den folgenden Instant Messaging-Clients (kurz: IM-Clients) kompatibel:

- iChat 4.0, 5.0 SL

Andere IM-Clients können möglicherweise für einfaches Instant Messaging verwendet werden, wurden jedoch für die Verwendung nicht zertifiziert.

Informationen zu den für die Verschlüsselung verwendeten Schlüsseln

Jedes Mal, wenn Sie sich bei der IM-Software anmelden, wird ein RSA-Schlüssel mit 1024 Bit erstellt. Wenn Sie sich abmelden, wird dieser Schlüssel vernichtet. Dieser Schlüssel wird verwendet, um auf Zufallsbasis erzeugte Seed-Daten mit jedem Kommunikationspartner auszutauschen. Die Seed-Daten werden kombiniert und ein Hash wird angewendet, damit jeder Kommunikationsteilnehmer einen Satz symmetrischer Schlüssel erstellen kann, der für diese bestimmte Kommunikation verwendet wird (ein Schlüssel pro Richtung). Mit den symmetrischen Schlüsseln werden alle Nachrichten mit AES-256 verschlüsselt.

Ein Teil dieser Daten wird auch genutzt, um einen HMAC (Keyed-Hash Message Authentication Code) für jede Nachricht zu erstellen, damit die Integrität der Nachricht geprüft werden kann.

Hinweis: Die für sichere IM-Kommunikation verwendeten Schlüssel können nicht vom Benutzer konfiguriert werden.

IM-Sitzungen verschlüsseln

Wenn die in *Informationen zur Instant Messaging-Kompatibilität von PGP Desktop* (auf Seite 139) beschriebenen Bedingungen erfüllt sind, beginnen Sie Ihre IM-Sitzung ganz normal. IM-Sitzungen mit anderen PGP Desktop-Benutzern, die einen kompatiblen IM-Client verwenden, werden automatisch und transparent geschützt.

Es gibt verschiedene Methoden, um zu überprüfen, ob die IM-Sitzung geschützt ist:

- Beim Start einer IM-Sitzung wird eine Benachrichtigung von PGP Notifier angezeigt, dass eine gesicherte IM-Sitzung gestartet wurde.

- Wenn die IM-Sitzung beginnt, wird unterhalb der ersten Nachricht des anderen Benutzers der Sitzung zusätzlicher Text angezeigt, dass eine mit PGP Desktop verschlüsselte Konversation begonnen hat.
- Wenn Sie das PGP-Protokoll nach dem Start der IM-Sitzung öffnen, werden Einträge angezeigt, dass ein Proxy für die IM-Sitzung verwendet wird, dass die Sitzung verschlüsselt wird usw. Dies können Sie dem folgenden Beispiel entnehmen:

  ```
  2006-09-15 11:39:49 AIM-Verbindung von AliceIM wird
  über Proxy mit Apple iChat abgewickelt.

  Die mit PGP Desktop verschlüsselte AIM-Sitzung mit
  JMedinaX wird initialisiert. Hierbei wird Ihr Schlüssel
  mit der ID 0x0910D29E verwendet.

  Verschlüsselte AIM-Sitzung mit JMedinaX wurde
  eingerichtet.
  ```

10 E-Mail-Nachrichten mit PGP Viewer anzeigen

In diesem Abschnitt finden Sie Informationen zum Verwenden von PGP Desktop zum Entschlüsseln, Verifizieren und Anzeigen von entschlüsselten Nachrichten mit PGP Viewer.

Hinweis: PGP Viewer wird nur auf Systemen ausgeführt, auf denen PGP Desktop installiert ist. PGP Viewer kann nicht als eigenständige Anwendung verwendet werden.

In diesem Kapitel

Übersicht über PGP Viewer 143
Verschlüsselte E-Mail-Nachrichten oder Dateien öffnen 145
E-Mail-Nachrichten in den Posteingang kopieren 146
E-Mail-Nachrichten exportieren 146
Einstellungen von PGP Viewer 147
Sicherheitsfunktionen in PGP Viewer 148

Übersicht über PGP Viewer

Bei normaler Verwendung befindet sich PGP Desktop zwischen dem E-Mail-Client (z. B. Mozilla Thunderbird) und dem E-Mail-Server, um ausgehende Nachrichten zu verschlüsseln und zu signieren und eingehende Nachrichten zu entschlüsseln und zu verifizieren. Bei dieser Funktionsweise wird PGP Desktop „im E-Mail-Strom“ eingesetzt.

Mit PGP Viewer können Sie Nachrichten *außerhalb* des E-Mail-Stroms entschlüsseln, verifizieren und anzeigen.

Es gibt verschiedene Gründe, warum Sie verschlüsselte Nachrichten ggf. außerhalb des E-Mail-Stroms erhalten haben:

- **Sicher gespeicherte verschlüsselte Nachrichten:** Viele Organisationen speichern Nachrichten aus Sicherheitsgründen verschlüsselt. Durch das Speichern befinden sie sich außerhalb des E-Mail-Stroms, jedoch können sie von PGP Viewer entschlüsselt, verifiziert und angezeigt werden, wobei die ursprüngliche verschlüsselte Nachricht beibehalten wird.

- **Verschlüsselter Text in einer Webmail-Nachricht:** An ein Webmail-Konto gesendete verschlüsselte Nachrichten können von PGP Desktop nicht entschlüsselt werden. Diese Nachrichten können jedoch von PGP Viewer entschlüsselt werden. Öffnen Sie die Dateianlage message.pgp mit PGP Viewer oder kopieren Sie den verschlüsselten Text und fügen Sie ihn in PGP Viewer ein.
- **Verschlüsselter Text, der nicht von PGP Desktop entschlüsselt wurde:** Wenn eine Nachricht vom E-Mail-Client automatisch heruntergeladen wurde, als PGP Desktop nicht ausgeführt wurde oder Ihre Passphrase nicht zwischengespeichert war, erhalten Sie möglicherweise verschlüsselten Nachrichtentext außerhalb des E-Mail-Stroms.

Mit PGP Viewer können verschiedene Arten von Messaging-Inhalt entschlüsselt, verifiziert und angezeigt werden:

- Aktueller mit einer PGP-Anwendung verschlüsselter Inhalt (PGP/MIME und PGP-partitioniert)
- Älterer mit einer PGP-Anwendung verschlüsselter Inhalt (PGP/MIME und PGP-partitioniert)
- Mit RFC-2822 kompatibler verschlüsselter Inhalt

PGP Viewer verwendet Schlüsselbunde von PGP Desktop für Vorgänge, die Schlüssel erfordern.

PGP Viewer behält entsprechende Einstellungen von PGP Desktop bei, z. B. Optionen zum Zwischenspeichern von Passphrasen.

In einer von einem PGP Universal Server verwalteten Umgebung sucht PGP Viewer anhand der jeweiligen Richtlinie nach Verifizierungsschlüsseln.

PGP Viewer zeigt Signaturinformationen für Nachrichten, die von PGP Viewer entschlüsselt wurden, im Nachrichtenfenster und nicht in der eigentlichen Nachricht an. Dadurch wird der Zugriff auf vollständige Signaturinformationen ermöglicht und das Spoofing von Inline-Signaturanmerkungen verhindert.

Unterstützte E-Mail-Clients

Mit PGP Viewer können Sie den Text einer entschlüsselten/verifizierten Nachricht in die folgenden E-Mail-Clients kopieren:

- Windows Mail (Windows)
- Microsoft Outlook (Windows)
- Thunderbird (Windows und Mac OS X)
- Outlook Express (Windows)
- Lotus Notes (Windows)
- Mail.app (Mac OS X)

Aufgrund des Designs der Architektur von Lotus Notes kann eine verschlüsselte Nachricht nicht zum Entschlüsseln aus dem Lotus Notes-E-Mail-Client in PGP Viewer gezogen werden.

Verschlüsselte E-Mail-Nachrichten oder Dateien öffnen

Mit PGP Viewer können Sie folgende Arten von verschlüsselten Nachrichtendateien öffnen (entschlüsseln, verifizieren und anzeigen):

- **.pgp:** Wurde mit einer PGP-Anwendung erstellt.
- **.eml:** Wurde mit Outlook Express oder Thunderbird erstellt.
- **.emlx:** Wurde unter Mac OS X mit dem E-Mail-Programm mail.app von Apple erstellt.
- **.msg:** Wurde mit Microsoft Outlook erstellt.

Wenn PGP Viewer eine verschlüsselte Nachricht öffnet, wird der verschlüsselte Text *nicht* überschrieben. Die Originalnachricht bleibt erhalten.

So können Sie eine verschlüsselte Nachricht aus einer Datei entschlüsseln, verifizieren und anzeigen

1. Öffnen Sie PGP Desktop und klicken Sie auf die Registerkarte „PGP Viewer“.
2. Klicken Sie auf **Datei in PGP Viewer öffnen** oder wählen Sie **Viewer > Datei in PGP Viewer öffnen** aus.
3. Wechseln Sie im Dialogfeld **Nachrichtendatei öffnen** zur gewünschten Datei, wählen Sie sie aus und klicken Sie auf **Öffnen**. Die Nachricht wird von PGP Viewer in einem separaten Fenster entschlüsselt, verifiziert und angezeigt.

   Hinweis: Sie können die Datei, die Sie entschlüsselt möchten, in den Bereich des PGP Viewer-Bildschirms ziehen, in dem Folgendes angezeigt wird: **E-Mail-Nachricht oder Dateien hier ablegen**. PGP Viewer öffnet die Datei, entschlüsselt und verifiziert sie und zeigt die Nachricht an.
4. Wenn Sie eine andere Nachricht öffnen möchten, klicken Sie in der Symbolleiste auf **Nachricht öffnen**, wechseln Sie zur gewünschten Datei, wählen Sie sie aus und klicken Sie auf **Öffnen**. PGP Viewer entschlüsselt und verifiziert die Nachricht und zeigt sie an.
5. Klicken Sie auf **Kleiner** oder auf **Größer**, um Text kleiner bzw. größer anzuzeigen.
6. Klicken Sie auf **Rich Text**, um die Nachricht oder Datei im Rich-Text-Format (RTF) anzuzeigen, oder auf **Klartext**, um sie als Klartext anzuzeigen.
7. Klicken Sie auf **Drucken**, um die Nachricht oder Datei zu drucken.

E-Mail-Nachrichten in den Posteingang kopieren

Mit PGP Viewer können Sie die Klartextversionen von entschlüsselten Nachrichten in den Posteingang des E-Mail-Clients kopieren.

So kopieren Sie eine Nachricht in den Posteingang des E-Mail-Clients

1. Wenn die gewünschte Nachricht im Fenster von PGP Viewer angezeigt wird, klicken Sie auf **In Posteingang kopieren**.

   Das Bestätigungsdialogfeld für **In Posteingang kopieren** wird angezeigt. Wenn diese Bestätigung künftig nicht mehr angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Nicht erneut anzeigen**.

   Im Bestätigungsdialogfeld **In Posteingang kopieren** wird der Name des E-Mail-Clients angezeigt, auf den die Nachricht kopiert wird. Informationen zum Ändern dieser Einstellung finden Sie unter „Einstellungen von PGP Viewer“.

2. Klicken Sie auf **OK**, um fortzufahren.

   Wenn Sie zum ersten Mal eine Nachricht in den E-Mail-Client Mozilla Thunderbird kopieren, werden Sie aufgefordert, ein Add-On zu installieren.

3. Klicken Sie auf **Ja**, um das Add-On zu installieren, und folgen Sie den Anweisungen auf dem Bildschirm oder klicken Sie auf **Nein**. Sie müssen Thunderbird 2.0 oder höher verwenden, um das Add-On installieren zu können.

   PGP Viewer öffnet den E-Mail-Client und kopiert eine Klartextversion der Nachricht in den Posteingang.

E-Mail-Nachrichten exportieren

Verwenden Sie PGP Viewer, um eine entschlüsselte Nachricht in eine Datei zu exportieren.

So exportieren Sie eine Nachricht von PGP Viewer in eine Datei

1. Wenn die Nachricht im Fenster von PGP Viewer angezeigt wird, klicken Sie auf **Exportieren**.

2. Geben Sie im Dialogfeld **Nachrichtendatei exportieren** den gewünschten Dateinamen, den Speicherort und das Format für die Datei an. Klicken Sie dann auf **Exportieren**.

   PGP Viewer speichert die Datei am angegebenen Speicherort.

Einstellungen von PGP Viewer

PGP Viewer umfasst Einstellungen, über die bestimmte Funktionen gesteuert werden können.

So greifen Sie auf die Einstellungen von PGP Viewer zu

1. Öffnen Sie PGP Viewer oder verwenden Sie PGP Viewer zum Entschlüsseln, Verifizieren und Anzeigen einer Nachricht.
2. Öffnen Sie das Menü **PGP Viewer** und klicken Sie auf **Einstellungen**.

   Das Dialogfeld **Einstellungen** wird angezeigt.
3. Klicken Sie auf die Registerkarte **Allgemein** und legen Sie die folgenden Einstellungen fest:
   - **Benutzer muss Befehl „In Posteingang kopieren“ bestätigen**: Steuert, ob beim Kopieren von Text aus PGP Viewer in den Posteingang des E-Mail-Clients eine Aufforderung zur Bestätigung angezeigt wird. Die Einstellung ist standardmäßig aktiviert.
   - **Remotebilder automatisch laden**: Steuert, ob externe Ressourcen wie Bilder, CSS-Stylesheets oder iframe-Inhalt automatisch von PGP Viewer geladen werden. Die Einstellung ist standardmäßig deaktiviert, da dies ein Sicherheitsrisiko darstellen kann.
   - **E-Mail-Client**: Hier können Sie den E-Mail-Client angeben, in den PGP Viewer Inhalt kopiert. Die Standardeinstellung ist der standardmäßige E-Mail-Client des Systems (PGP Viewer ermittelt den standardmäßigen E-Mail-Client des Systems und verwendet diesen als Standardeinstellung). Sie können **Mail.app** oder **Thunderbird** auswählen.
4. Klicken Sie auf die Registerkarte **Schriftarten und Farben** und geben Sie die folgenden Einstellungen an:
   - **Schriftart**: Legt die Schriftart fest, die PGP Viewer zum Anzeigen von Text verwendet. Klicken Sie auf **Auswählen** und geben Sie die gewünschten Einstellungen für **Sammlung**, **Familie**, **Schriftart** und **Größe** an.
   - **Textfarbe**: Legt die Farbe fest, in der PGP Viewer Text anzeigt. Klicken Sie auf den Farbenblock und wählen Sie die gewünschte Farbe aus.
   - **Hintergrundfarbe**: Legt die Hintergrundfarbe von Text fest, die PGP Viewer anzeigt. Klicken Sie auf den Farbenblock und wählen Sie die gewünschte Farbe aus.

Sicherheitsfunktionen in PGP Viewer

PGP Viewer gewährleistet Ihre Sicherheit proaktiv:

- Für den in PGP Viewer eingebetteten Webbrowser, der Messaging-Inhalt anzeigt, sind JavaScript, Java-Applets und Plug-ins deaktiviert. Dadurch wird verhindert, dass ein Angreifer böswillige Nutzlast übermittelt, die von PGP Viewer andernfalls geladen würde.
- Externe Ressourcen wie Bilder, CSS-Stylesheets oder iframe-Inhalt (ein Inline-Frame, der ein anderes Dokument enthält) werden entsprechend der Einstellung **Remotebilder automatisch laden** automatisch geladen. Aus Sicherheitsgründen ist diese Einstellung standardmäßig deaktiviert. Wenn diese Einstellung deaktiviert ist, generiert PGP Viewer keinen Netzwerkverkehr zu externen Websites.

11 Laufwerke mit PGP Whole Disk Encryption schützen

PGP Whole Disk Encryption (PGP WDE) sperrt den gesamten Inhalt von Desktop- oder Laptop-Computern, externen Laufwerken und USB-Flash-Laufwerken, einschließlich Startsektoren, System- und Auslagerungsdateien. Die Verschlüsselung läuft für den Benutzer transparent im Hintergrund ab. Wichtige Daten werden automatisch geschützt, ohne dass weitere Eingriffe erforderlich sind.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat der PGP Universal Server-Administrator möglicherweise bestimmte Funktionen deaktiviert. Wenn eine Funktion deaktiviert wurde, wird das entsprechende Bedienelement auf der linken Seite nicht angezeigt und das Menü und andere Optionen für diese Funktion sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn der PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, hat der PGP-Administrator möglicherweise durch Richtlinie festgelegt, dass alle Startlaufwerke verschlüsselt werden müssen. In diesem Fall überprüft PGP Desktop in regelmäßigen Abständen, ob die Laufwerke verschlüsselt sind, und setzt die Richtlinie durch das automatische Verschlüsseln nicht verschlüsselter Startlaufwerke durch.

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, hat der PGP-Administrator möglicherweise durch Richtlinie festgelegt, dass alle Systemlaufwerke verschlüsselt werden müssen. In diesem Fall überprüft PGP Desktop in regelmäßigen Abständen, ob die Laufwerke verschlüsselt sind, und setzt die Richtlinie durch das automatische Verschlüsseln nicht verschlüsselter Systemlaufwerke durch.

In diesem Kapitel

Informationen zu PGP Whole Disk Encryption 150
PGP Whole Disk Encryption lizenzieren 153
Laufwerk auf die Verschlüsselung vorbereiten 153
Authentifizierungsmethode für das Laufwerk bestimmen 158
Laufwerke verschlüsseln 158
Mit PGP Whole Disk Encryption verschlüsselte Laufwerke verwenden 163
Schutz von Laufwerken aufrechterhalten 165
PGP Whole Disk Encryption in einer von einem PGP Universal Server verwalteten Umgebung verwenden 170
Daten von verschlüsselten Laufwerken wiederherstellen 172
Mit PGP Whole Disk Encryption verschlüsselte Laufwerke entschlüsseln 174
Wechseldatenträger auf anderen Systemen verwenden 175
Auf Daten auf verschlüsselten Wechseldatenträgern zugreifen 175
Spezielle Sicherheitsmaßnahmen von PGP Desktop 176
Technische Details zum Verschlüsseln von Startlaufwerken 178

Informationen zu PGP Whole Disk Encryption

Mit PGP Whole Disk Encryption können Sie das Startlaufwerk (nur von Intel-basierten Macintosh-Computern) und externe Laufwerke auf Mac OS X-Systemen vollständig verschlüsseln. Zudem können externe, unter Windows formatierte Laufwerke vollständig verschlüsselt werden.

Wichtig: Bei PGP Desktop 9.9 und höher wird eine andere Partitionierungsmethode als bei Versionen von PGP Desktop vor Version 9.9 verwendet. Wenn Sie PGP Whole Disk Encryption von PGP Desktop-Versionen vor Version 9.9 verwendet haben, müssen Sie die Laufwerke *vor* der Installation von Version 10.1 entschlüsseln. Andernfalls können Sie nicht mehr auf die darauf gespeicherten Daten zugreifen.

Wenn Sie ein ganzes Laufwerk mit PGP Whole Disk Encryption verschlüsseln, wird jeder Sektor mit einem symmetrischen Schlüssel verschlüsselt. Dies umfasst alle Dateien, einschließlich Betriebssystemdateien, Programmdateien, Datendateien, Auslagerungsdateien, freien Speicherplatz sowie temporäre Dateien.

Bei jedem nachfolgenden Systemstart werden Sie von PGP Whole Disk Encryption zur Eingabe der richtigen Passphrase aufgefordert. Die verschlüsselten Daten werden daraufhin entschlüsselt, wenn Sie auf sie zugreifen. Bevor Daten auf das Laufwerk geschrieben werden, verschlüsselt PGP Whole Disk Encryption diese Daten. Solange Sie für das mit PGP Whole Disk Encryption verschlüsselte Laufwerk authentifiziert sind (nach Eingabe der korrekten Passphrase im PGP BootGuard-Bildschirm), sind die Dateien verfügbar. Wenn Sie das System herunterfahren, ist das Laufwerk vor Verwendung durch andere Personen geschützt.

Wenn das System die Intel® Advanced Encryption Standard (AES) Instructions (AES-NI) unterstützt, wird das System mit der Hardware verschlüsselt und entschlüsselt, die diesem Verschlüsselungsalgorithmus zugeordnet ist. AES-NI bietet während des Verschlüsselungs- und Entschlüsselungsvorgangs erweiterte Leistung.

Es ist wichtig, dass Sie sich vor der Verschlüsselung des Laufwerks mit PGP Whole Disk Encryption bewusst sind, wie ein mit PGP Whole Disk Encryption verschlüsseltes Laufwerk erstellt und verwendet wird:

1 Stellen Sie sicher, dass die PGP Desktop-Lizenz die Verwendung der Funktion unterstützt (siehe *PGP Whole Disk Encryption lizenzieren* (auf Seite 153)).

2 Führen Sie die Schritte unter *Laufwerk auf die Verschlüsselung vorbereiten* (auf Seite 153) aus.

3 Wählen Sie die Authentifizierungsmethode zum Verschlüsseln des Laufwerks aus (siehe *Authentifizierungsmethode für das Laufwerk bestimmen* (auf Seite 158)).

4 Starten Sie den Verschlüsselungsvorgang (siehe *Laufwerke verschlüsseln* (auf Seite 158)).

5 Machen Sie sich mit der Verwendung eines verschlüsselten Laufwerks vertraut (siehe *Mit PGP Whole Disk Encryption verschlüsselte Laufwerke verwenden* (auf Seite 163)).

6 Machen Sie sich mit der Wartung des verschlüsselten Laufwerks vertraut (siehe *Schutz von Laufwerken aufrechterhalten* (auf Seite 165)).

7 Machen Sie sich damit vertraut, wie Sie das Laufwerk bei Bedarf entschlüsseln (siehe *Mit PGP Whole Disk Encryption verschlüsselte Laufwerke entschlüsseln* (auf Seite 174)).

8 Machen Sie sich mit den Funktionen vertraut, mit denen Sie Sicherheitsprobleme vermeiden können (siehe *Spezielle Sicherheitsmaßnahmen von PGP Desktop* (auf Seite 176)).

Wenn Sie ein PGP Universal Server-Administrator sind oder PGP Whole Disk Encryption in einer von einem PGP Universal Server verwalteten Umgebung verwenden, finden Sie weitere Informationen unter *PGP Whole Disk Encryption in einer von einem PGP Universal Server verwalteten Umgebung verwenden* (auf Seite 170).

Warnung: Nachdem Sie ein Laufwerk entsperrt haben, stehen die darauf befindlichen Dateien nicht nur Ihnen, sondern allen Personen zur Verfügung, die physischen Zugang zu dem System haben. Die Dateien bleiben so lange entsperrt, bis Sie den Computer herunterfahren und die Dateien dadurch wieder sperren. Verwenden Sie ein PGP Virtual Disk-Laufwerk für Dateien, die auch dann geschützt bleiben sollen, wenn Sie am Computer arbeiten. Weitere Informationen finden Sie unter *PGP Virtual Disk-Laufwerke verwenden* (auf Seite 181).

Startlaufwerke verschlüsseln

Ab PGP Desktop für Mac OS X Version 10.1 können Sie das Startlaufwerk eines auf Intel basierten Macintosh vollständig verschlüsseln. Wechseldatenträger und USB-Flash-Laufwerke können natürlich weiterhin wie mit den Versionen von PGP Desktop vor Version 10.1 verschlüsselt werden.

Wichtig: Boot Camp von Apple funktioniert nur, wenn PGP Desktop und Boot Camp von Apple in einer bestimmten Reihenfolge installiert werden. Weitere Informationen finden Sie unter *PGP Desktop mit Boot Camp von Apple verwenden* (auf Seite 20)

PGP Whole Disk Encryption unterstützt auf Intel basierten Mac OS X-Systemen sowohl 32 Bit als auch 64 Bit.

Hinweis: Die Mac OS X-Funktion zum sicheren Systemstart kann nicht bei einem vollständig verschlüsselten Startlaufwerk verwendet werden, da sie Kernel-Erweiterungen deaktiviert, die für PGP Whole Disk Encryption erforderlich sind. Wenn Sie nach der Authentifizierung im PGP BootGuard-Bildschirm die Umschalttaste gedrückt halten, wird das System *nicht* gestartet. Stattdessen wird nach ein paar Minuten ein Neustart durchgeführt.

Worin unterscheidet sich PGP Whole Disk Encryption von PGP Virtual Disk?

Der Unterschied zwischen PGP Virtual Disk und PGP Whole Disk Encryption liegt darin, dass sich PGP Virtual Disk-Laufwerke wie zusätzliche Laufwerke im System verhalten, die auch dann gesperrt werden können, wenn Sie am Computer arbeiten. Diese Laufwerke sind mit einem Tresor vergleichbar, in dem Dateien aufbewahrt werden, die geschützt werden müssen. Es handelt sich dabei nicht um ein physisches, sondern um ein virtuelles Laufwerk, das mit PGP Virtual Disk erstellt und verwaltet wird.

PGP Whole Disk Encryption schützt die gesamte physische Festplatte.

Beide Produkte arbeiten unabhängig voneinander und können daher gleichzeitig eingesetzt werden. Weitere Informationen finden Sie unter *PGP Virtual Disk-Laufwerke verwenden* (auf Seite 181).

PGP Whole Disk Encryption lizenzieren

Damit Sie PGP Whole Disk Encryption verwenden können, muss Ihre Kopie von PGP Desktop über eine Lizenz verfügen, die diese Funktion unterstützt.

So überprüfen Sie, ob die Lizenz PGP Whole Disk Encryption unterstützt

1. Öffnen Sie PGP Desktop.
2. Klicken Sie im Menü **PGP** auf **Lizenz**. Das Dialogfeld mit den Lizenzinformationen wird angezeigt.
3. Klicken Sie auf **Details**. Die Details der Lizenz werden angezeigt. Vergewissern Sie sich im Abschnitt „Aktivierte Funktionen“, dass **PGP Whole Disk Encryption** aufgeführt ist.

Wenn PGP Whole Disk Encryption von der Lizenz nicht unterstützt wird, können Sie mit einem der folgenden Verfahren weitere Informationen zur Lizenzierung von PGP Desktop abrufen:

- Falls Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, erhalten Sie Informationen zur Unterstützung von PGP Whole Disk Encryption im Rahmen Ihrer Lizenz vom PGP-Administrator. Weitere Informationen finden Sie unter *PGP Desktop mit PGP Universal Server verwenden* (auf Seite 239).
- Falls Sie PGP Desktop nicht in einer von einem PGP Universal Server verwalteten Umgebung verwenden, finden Sie auf der *Website der PGP Corporation* (*http://www.pgp.com*) Informationen zum Erweitern der Lizenz um PGP Whole Disk Encryption.

Ablauf der Lizenz

Wenn PGP Whole Disk Encryption unter einer Mietlizenz verwendet wird, steht nach Ablauf der Lizenz noch 90 Tage ausschließlich für Startlaufwerke eine Entschlüsselungsfunktion zur Verfügung. 90 Tage nach Ablauf der Mietlizenz werden Ihre Daten von PGP Whole Disk Encryption entschlüsselt (nach einer entsprechenden Benachrichtigung), damit Sie auf Ihre Dateien zugreifen können.

Laufwerk auf die Verschlüsselung vorbereiten

Vor der Verschlüsselung des Laufwerks müssen Sie einige Schritte ausführen, damit die erste Verschlüsselung des Laufwerks erfolgreich abläuft.

- **Vergewissern Sie sich, dass das Ziellaufwerk unterstützt wird.** Weitere Informationen finden Sie unter *Unterstützte Laufwerkstypen* (auf Seite 154).
- **Stellen Sie sicher, dass Sie für die Passphrase nur unterstützte Zeichen verwenden.** Weitere Informationen finden Sie unter *Unterstützte Zeichen* (auf Seite 159).
- **Stellen Sie vor dem Verschlüsseln sicher, dass sich das Laufwerk in einwandfreiem Zustand befindet.** Falls PGP Whole Disk Encryption während der Verschlüsselung Laufwerksfehler erkennt, wird die Verschlüsselung angehalten, damit die Probleme behoben werden können. Es ist jedoch effizienter, Fehler vor dem Beginn der Verschlüsselung zu beheben. Weitere Informationen finden Sie unter *Laufwerksintegrität vor der Verschlüsselung sicherstellen* (auf Seite 156).
- **Sichern Sie das Laufwerk, bevor Sie es verschlüsseln.** Sichern Sie das Laufwerk vor der Verschlüsselung, damit keine Daten verloren gehen, wenn der Laptop oder Computer verloren geht, gestohlen wird oder Sie das Laufwerk nicht entschlüsseln können. Zudem sollten Sie regelmäßig Sicherungskopien des Laufwerks anlegen.
- **Berücksichtigen Sie, wie lange die Verschlüsselung des Laufwerks dauern wird**, und bereiten Sie sich entsprechend vor. Weitere Informationen finden Sie unter *Verschlüsselungsdauer berechnen* (auf Seite 157).
- **Führen Sie einen Pilotversuch durch, um die Softwarekompatibilität sicherzustellen.** Die PGP Corporation empfiehlt, PGP Whole Disk Encryption zur Sicherheit auf einer kleinen Gruppe von Computern zu testen, um sicherzustellen, dass kein Konflikt zwischen PGP Whole Disk Encryption und anderer auf dem Computer installierter Software besteht. Erst dann sollte die Funktion auf einer großen Anzahl von Computern bereitgestellt werden. Dies bietet sich besonders in Umgebungen an, in denen ein standardisiertes COE-Image (Corporate Operating Environment) verwendet wird. Es gibt bestimmte andere Software für den Laufwerksschutz, die nicht mit PGP Whole Disk Encryption kompatibel ist und schwerwiegende Laufwerksprobleme verursachen kann, einschließlich Datenverlust. Informationen zu bekannten Interoperabilitätsproblemen finden Sie unter *Pilotversuch zum Sicherstellen der Softwarekompatibilität durchführen* (auf Seite 157). Aktuelle Informationen zu kompatibler Software finden Sie in den *Versionshinweisen zu PGP Desktop*.
- **Stellen Sie sicher, dass der Standbymodus deaktiviert ist.** PGP Desktop ist nicht mit dem Ruhemodus von Mac OS X-Systemen kompatibel.

Unterstützte Laufwerkstypen

Mit PGP Whole Disk Encryption kann der Inhalt folgender Arten von Laufwerken geschützt werden:

- Desktop- oder Laptop-Laufwerke, einschließlich Solid-State-Laufwerke

  Hinweis: Verwenden Sie PGP Whole Disk Encryption nicht zur Verschlüsselung von Serverhardware. PGP Whole Disk Encryption wird nicht von Mac OS X-Serverhardware unterstützt.

- Externe Laufwerke, *mit Ausnahme von* Musikgeräten und Digitalkameras
- USB-Flash-Laufwerke, die auch als USB-Sticks bezeichnet werden

Mit PGP Whole Disk Encryption können Laufwerke beliebiger Größe verschlüsselt werden. Wenn das Laufwerk vom Betriebssystem (oder vom Hardware-BIOS des Startlaufwerks) unterstützt wird, sollte das Laufwerk mit PGP Desktop kompatibel sein.

Wenn Sie eine Partitionierung eines mit PGP Whole Disk Encryption verschlüsselten Laufwerks ausführen möchten, müssen Sie das Laufwerk zunächst entschlüsseln. Nachdem Sie das Laufwerk entschlüsselt haben, können Sie die Partitionierung vornehmen.

PGP Whole Disk Encryption unterstützt alle Mac OS X-Energieverwaltungsmodi.

Nicht unterstützte Laufwerkstypen

Folgende Laufwerkstypen werden *nicht* unterstützt:

- Mit der APM-Partitionierungsmethode formatierte Laufwerke
- Beliebige Serverhardware, einschließlich RAID-Laufwerke
- Disketten und CD-RW/DVD-RWs

Unterstützte Tastaturen

Im PGP Whole Disk Encryption-Anmeldebildschirm werden folgende Tastaturlayouts unterstützt:

- Englisch (USA, International)
- Japanisch (Japan)
- Deutsch (Deutschland)
- Französisch (Frankreich)
- Spanisch (Lateinamerika)
- Spanisch (Spanien, ISO)

Bei den verschiedenen Tastaturlayouts können Zeichen unterschiedlichen Tasten zugeordnet sein. Dies kann bei der Eingabe der Passphrase zu Problemen führen. Stellen Sie sicher, dass Sie das unterstützte Tastaturlayout angeben (unter „Systemeinstellungen“ > „Persönlich“ > „Landeseinstellungen“) und verwenden Sie immer dieses Layout für die Authentifizierung.

Hinweis: Die Namen der Tastaturen können in den verschiedenen Sprachen unterschiedlich sein. Wenn „Englisch (USA, International)“ in PGP BootGuard nicht funktioniert, wählen Sie „USA“ aus.

Laufwerksintegrität vor der Verschlüsselung sicherstellen

Die PGP Corporation nimmt bei der Laufwerksverschlüsselung bewusst eine konservative Haltung ein, um Datenverlust zu verhindern. Bei der Verschlüsselung von Festplatten treten nicht selten Fehler bei der zyklischen Redundanzprüfung auf. Wenn PGP Whole Disk Encryption eine Festplatte mit fehlerhaften Sektoren erkennt, wird der Verschlüsselungsvorgang standardmäßig unterbrochen. Während dieser Zeit können Sie das Problem beheben, bevor Sie den Verschlüsselungsvorgang fortsetzen. Auf diese Weise werden mögliche Laufwerksbeschädigungen und Datenverluste verhindert.

Damit es während der Verschlüsselung nicht zu einer Unterbrechung kommt, empfiehlt die PGP Corporation, vor der Verschlüsselung alle Laufwerksfehler zu korrigieren.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, werden die bei der Verschlüsselung erkannten fehlerhaften Sektoren im PGP Universal Server aufgezeichnet und der Verschlüsselungsvorgang wird fortgesetzt.

Empfehlungen für bewährte Methoden

Bevor Sie versuchen, PGP Whole Disk Encryption einzusetzen, sollten Sie ein Laufwerk-Scanprogramm eines Drittanbieters verwenden, um eine Integritätsprüfung auf niedriger Stufe durchzuführen und alle Unregelmäßigkeiten des Laufwerks zu reparieren, die zu Fehlern bei der zyklischen Redundanzprüfung führen könnten. Diese Softwareanwendungen können Fehler korrigieren, die ansonsten die Verschlüsselung unterbrechen würden.

Wenn Sie Boot Camp von Apple verwenden, empfiehlt die PGP Corporation, sämtliche Verschlüsselungs- und Entschlüsselungsvorgänge auf der Mac OS X-Partition auszuführen. Achten Sie darauf, dass Sie PGP Desktop sowohl auf der Mac OS X- als auch auf der Windows-Partition installiert haben. Starten Sie erst dann die Mac OS X-Partition, um eine Verschlüsselung oder Entschlüsselung vorzunehmen.

Achtung: Stark fragmentierte Laufwerke sollten vor ihrer Verschlüsselung defragmentiert werden.

Verschlüsselungsdauer berechnen

Die Verschlüsselung ist zeitaufwändig und CPU-intensiv. Je größer das zu verschlüsselnde Laufwerk ist, desto länger dauert der Vorgang. Beachten Sie dies, wenn Sie die erstmalige Verschlüsselung des Laufwerks planen.

Die folgenden Faktoren können sich auf die Verschlüsselungsgeschwindigkeit auswirken:

- Größe des Laufwerks
- Prozessorgeschwindigkeit und Anzahl der Prozessoren
- Anzahl der auf dem Computer ausgeführten Systemprozesse
- Anzahl der auf dem Computer ausgeführten anderen Anwendungen
- Prozessorzeit für diese anderen Anwendungen

Auf einem durchschnittlichen System dauert die Verschlüsselung eines 80-GB-Startlaufwerks mit PGP Whole Disk Encryption ca. drei Stunden (wenn keine anderen Anwendungen ausgeführt werden). Auf einem sehr schnellen System kann diese Verschlüsselung hingegen in weniger als einer Stunde durchgeführt werden.

Sie können das System während der Verschlüsselung weiterhin verwenden. Das System arbeitet zwar während des Verschlüsselungsvorgangs etwas langsamer als gewöhnlich, kann jedoch uneingeschränkt verwendet werden.

PGP Desktop verlangsamt die Verschlüsselung automatisch, wenn Sie das System verwenden. Wenn Sie das System während der ersten Verschlüsselung nicht verwenden, wird der Verschlüsselungsvorgang schneller durchgeführt. Nach der Verschlüsselung arbeitet das System wieder mit normaler Geschwindigkeit.

Wenn Sie während des Verschlüsselungsvorgangs andere Anwendungen nutzen, werden diese wahrscheinlich etwas langsamer als gewohnt ausgeführt, bis die Verschlüsselung abgeschlossen ist.

Pilotversuch zum Sicherstellen der Softwarekompatibilität durchführen

Die PGP Corporation empfiehlt, PGP Whole Disk Encryption zur Sicherheit auf einer kleinen Gruppe von Computern zu testen, um sicherzustellen, dass kein Konflikt zwischen PGP Whole Disk Encryption und anderer auf dem Computer installierter Software besteht. Erst dann sollte die Funktion auf einer großen Anzahl von Computern bereitgestellt werden.

Authentifizierungsmethode für das Laufwerk bestimmen

Wenn Sie ein Laufwerk mit PGP Whole Disk Encryption verschlüsseln, legen Sie fest, wie Sie sich selbst zum Entschlüsseln des Laufwerks oder der Partition authentifizieren.

Sie haben folgende Möglichkeiten:

- **Passphrase:** Bei der Authentifizierung mit einer Passphrase geben Sie beim Verschlüsseln eines Laufwerks eine Passphrase an. Beim Zugriffsversuch auf das verschlüsselte Laufwerk müssen Sie diese Passphrase eingeben.
- **Öffentlicher Schlüssel:** Bei der Authentifizierung mit einem öffentlichen Schlüssel geben Sie beim Verschlüsseln eines Laufwerks einen öffentlichen Schlüssel an. Nur der Inhaber des entsprechenden privaten Schlüssels kann auf den Inhalt des Laufwerks zugreifen. Zu diesem Zweck muss der Benutzer die Passphrase seines privaten Schlüssels eingeben. Die Authentifizierung mit öffentlichen Schlüsseln ist nur für Wechseldatenträger verfügbar, die mit dem System verwendet werden. Festplatten (auch Startlaufwerke oder externe USB-Festplatten) müssen mithilfe eines Passphrasenbenutzers verschlüsselt werden.

Bei der erstmaligen Verschlüsselung eines *Startlaufwerks* können Sie nur die Authentifizierung mit einer Passphrase als Authentifizierungsmethode auswählen. Nach der erstmaligen Verschlüsselung können Sie weitere Passphrasenbenutzer für das Laufwerk hinzufügen.

Während der erstmaligen Verschlüsselung eines *nicht zum Starten verwendeten Laufwerks* (z. B. einer externen Festplatte) können Sie zwischen der Authentifizierung mit einer Passphrase oder mit einem öffentlichen Schlüssel auswählen.

Laufwerke verschlüsseln

Nachdem Sie das Laufwerk vorbereitet haben, können Sie es verschlüsseln. Beachten Sie zuvor folgende Punkte:

- Das System arbeitet zwar während des Verschlüsselungsvorgangs etwas langsamer als gewöhnlich, kann jedoch uneingeschränkt verwendet werden. Nach der Verschlüsselung arbeitet es wieder mit normaler Geschwindigkeit.

  PGP Desktop verlangsamt die Verschlüsselung automatisch, wenn Sie das System verwenden. Wenn Sie das System während der ersten Verschlüsselung nicht verwenden, wird der Verschlüsselungsvorgang schneller durchgeführt.

- Sie können PGP Desktop während der Verschlüsselung minimieren oder schließen. Dies hat keine Auswirkungen auf den Prozess, erhöht jedoch die Geschwindigkeit des Verschlüsselungsvorgangs.
- Unterbrechen Sie die Verschlüsselung vorübergehend, indem Sie auf **Anhalten** und danach im Dialogfeld auf **Pause** klicken. Klicken Sie auf **Fortsetzen**, um den Vorgang wieder zu starten. Nachdem Sie auf **Fortsetzen geklickt haben, müssen Sie sich möglicherweise authentifizieren.**
- Wenn Sie das System vor Abschluss des Verschlüsselungsvorgangs herunterfahren möchten, fahren Sie es normal herunter. Sie müssen die Verschlüsselung dazu nicht anhalten. Beim nächsten Systemstart wird der Verschlüsselungsvorgang automatisch an dem Punkt fortgesetzt, an dem er unterbrochen wurde.

Sie können jeweils immer nur ein Laufwerk verschlüsseln, entschlüsseln bzw. umschlüsseln. Wenn Sie eine dieser Operationen für ein Laufwerk starten, können Sie erst nach Abschluss der ersten Operation einen weiteren Verschlüsselungsvorgang beginnen. Dies kann auch nicht durch Anhalten der ersten Operation umgangen werden.

Unterstützte Zeichen

PGP Whole Disk Encryption unterstützt beim Erstellen von Passphrasen alphanumerische Zeichen, Interpunktionszeichen und Standard-Metazeichen. Tabulatorzeichen und Steuerzeichen werden nicht unterstützt. Beachten Sie bei der Auswahl einer Passphrase die folgenden Punkte.

Die folgenden Zeichen werden unterstützt:
`abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ`

`0123456789`

`` `~!@#$%^&*()_+={}\|:;[]'"<>,.?/- ``

Die meisten Zeichen des erweiterten ASCII-Zeichensatzes (z. B. `ç é è ê ë î ï ô û ù ü ÿ`) oder Symbole (z. B. `¢ ® œ`) werden unterstützt.

Laufwerk verschlüsseln

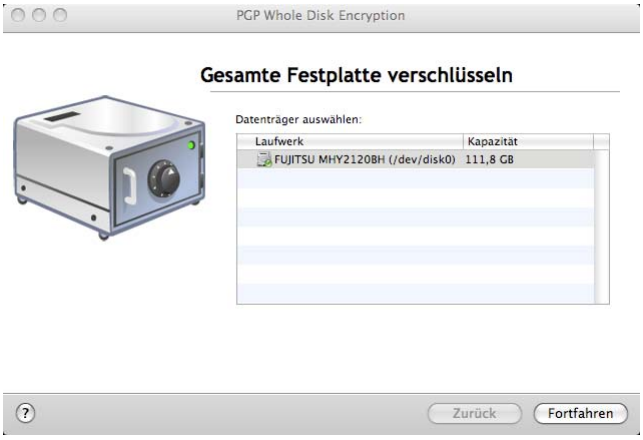
Sichern Sie das Laufwerk vor der Verschlüsselung, damit keine Daten verloren gehen, wenn der Laptop oder Computer verloren geht, gestohlen wird oder Sie das Laufwerk nicht entschlüsseln können.

Achtung: Installieren Sie während der Verschlüsselung des Laufwerks keine möglicherweise verfügbaren Betriebssystemaktualisierungen. Falls die Aktualisierung automatisch erfolgt, starten Sie den Computer erst nach Abschluss des Verschlüsselungsvorgangs neu.

So schützen Sie ein Laufwerk mit PGP Whole Disk Encryption

1 Öffnen Sie PGP Desktop und klicken Sie auf „PGP Disk“. Der PGP Disk-Bildschirm wird angezeigt.

2 Klicken Sie auf **Gesamte Festplatte verschlüsseln**. Der Bildschirm „Gesamte Festplatte verschlüsseln“ wird angezeigt. Hier sind alle Laufwerke des Systems aufgeführt, die geschützt werden können.



3 Wählen Sie aus der Liste **Datenträger auswählen** **das Laufwerk aus, das Sie schützen möchten.**

4 Legen Sie im Bereich **Sichern mit** fest, wie Sie auf das geschützte Laufwerk zugreifen möchten: Sie können zwischen einem **Benutzer öffentlicher Schlüssel** und einem **Passphrasenbenutzer** auswählen.

Hinweis: Wenn Sie ein Startlaufwerk verschlüsseln, können Sie nur die Authentifizierung mit einer Passphrase verwenden. Daher wählt PGP Desktop automatisch die Option für Passphrasenbenutzer aus und wechselt direkt zum Bildschirm „Benutzer von PGP Whole Disk hinzufügen“.

- Wenn Sie das Laufwerk mit einem öffentlichen Schlüssel schützen möchten, wählen Sie **Öffentlicher Schlüssel** aus und klicken Sie auf **Fortfahren**. Der Bildschirm „Benutzer von PGP Whole Disk hinzufügen“ wird angezeigt. Diese Option steht nicht zur Verfügung, wenn Sie das Laufwerk bereits verschlüsselt haben.

  Wählen Sie einen Schlüssel aus der Liste aus und klicken Sie auf **Fortfahren**. Das Dialogfeld „PGP-Passphrase eingeben“ wird angezeigt.

  Geben Sie die Passphrase für den ausgewählten Schlüssel ein und klicken Sie auf **OK**. Der Bildschirm „Übersicht über PGP Whole Disk Encryption“ wird angezeigt mit Informationen darüber, wie das Laufwerk verschlüsselt wird, welcher Schlüssel verwendet wird usw.

- Wenn Sie das Laufwerk mit einer Passphrase schützen möchten, wählen Sie **Passphrase** **aus und klicken Sie auf Fortfahren. Der Bildschirm „Benutzer von PGP Whole Disk hinzufügen“ wird angezeigt.**

  Geben Sie im Feld **Name** einen Namen ein oder übernehmen Sie den Standardnamen. Geben Sie im Feld **Passphrase eingeben** die Passphrase ein und nehmen Sie dieselbe Eingabe erneut im Feld **Passphrase bestätigen** **vor. Wenn die Zeichen während der Eingabe der Passphrase angezeigt werden sollen, wählen Sie Tastatureingabe anzeigen aus.**

  Die Passphrasen-Qualitätsanzeige kann als allgemeiner Anhaltspunkt für die Stärke der erstellten Passphrase verwendet werden. Dabei wird der Entropiewert der eingegebenen Passphrase mit einer echten zufälligen Zeichenkette mit 128 Bit verglichen. Dies entspricht dem Entropiewert eines AES-128-Schlüssels. Weitere Informationen finden Sie unter *Die Passphrasen-Qualitätsanzeige* (auf Seite 234).

5 Klicken Sie auf **Fortfahren**. Der Bildschirm „Übersicht über PGP Whole Disk Encryption“ wird angezeigt mit Informationen darüber, wie das Laufwerk verschlüsselt wird, welcher Schlüssel verwendet wird usw.

6 Überprüfen Sie die angezeigten Informationen. Wenn Sie die Option **Stromausfallschutz** aktivieren möchten, aktivieren Sie das Kontrollkästchen.

Die erstmalige Verschlüsselung kann jederzeit unterbrochen werden, indem der Computer ordnungsgemäß heruntergefahren oder neu gestartet wird. Es sollte jedoch unbedingt vermieden werden, dass der Computer unerwartet abgeschaltet wird, z. B. durch Stromausfall, versehentliches Herausziehen des Netzkabels usw. Wenn dies nicht völlig ausgeschlossen werden kann oder wenn keine unterbrechungsfreie Stromversorgung zur Verfügung steht, sollten Sie eventuell die Option „Stromausfallschutz“ auswählen. Wenn die Option „Stromausfallschutz“ aktiviert ist, wird die Verschlüsselung im Journal erfasst. Auf diese Weise kann der Verschlüsselungsvorgang nach einer Unterbrechung der Stromversorgung sicher und zuverlässig fortgesetzt werden. Allerdings kann die erstmalige Verschlüsselung mit dieser Option um ein Vielfaches länger dauern.

Diese Option bietet sich auch bei der Verschlüsselung von USB-Geräten an. Sollte die Verschlüsselung unterbrochen werden, indem das USB-Gerät während der Verschlüsselung entfernt wird, kann das Gerät beschädigt werden und muss gegebenenfalls neu formatiert werden. Die Verschlüsselung im Modus für den Stromausfallschutz ermöglicht Ihnen, das USB-Gerät während der Verschlüsselung zu entfernen und mit der Verschlüsselung fortzufahren, nachdem es wieder angeschlossen wurde.

7 Klicken Sie auf **Verschlüsseln**. Der Verschlüsselungsvorgang beginnt und der Bildschirm „Verschlüsselungsfortschritt“ wird angezeigt.

8 Klicken Sie auf **Schließen**. Der PGP Desktop-Bildschirm wird angezeigt, während der Verschlüsselungsvorgang im Hintergrund fortgesetzt wird. In einer Fortschrittsanzeige wird der Fortgang der Verschlüsselung angezeigt.

Hinweis: Der Verschlüsselungsvorgang wird fortgesetzt, auch wenn Sie den Bildschirm „Verschlüsselungsfortschritt“ schließen. Die Fortschrittsanzeige wird jedoch erst angezeigt, wenn Sie diesen Bildschirm schließen.

9 Während des Verschlüsselungsvorgangs haben Sie folgende Möglichkeiten:

- Wenn Sie den Vorgang vorübergehend unterbrechen möchten, klicken Sie auf **Anhalten**. Daraufhin wird das Dialogfeld „Verschlüsselung nicht abgeschlossen“ angezeigt.
- Sie können den Vorgang mit **Pause** anhalten, den Bereich des bereits verschlüsselten Laufwerks mit **Entschlüsseln** wieder entschlüsseln oder das Dialogfeld mit **Abbrechen** schließen, um den Verschlüsselungsvorgang fortzusetzen.

Hinweis: Wenn der Verschlüsselungsvorgang unterbrochen wird und PGP Desktop einen Lese-/Schreibfehler meldet, wurden von PGP Desktop fehlerhafte Sektoren auf dem Laufwerk erkannt. Machen Sie in diesem Fall die Verschlüsselung sofort rückgängig, indem Sie den bereits verschlüsselten Bereich des Laufwerks *entschlüsseln*. Verwenden Sie anschließend ein Programm für die Laufwerksprüfung, um nach dem Problem zu suchen und es zu beheben.

Wenn der Verschlüsselungsvorgang abgeschlossen ist, werden die Laufwerkseigenschaften des verschlüsselten Laufwerks angezeigt. Dazu zählen u. a. Beschreibung, Typ des Laufwerks, Größe, verschlüsselter Status und Informationen zum Benutzerzugriff.

Laufwerksfehler während der Verschlüsselung

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, werden die bei der Verschlüsselung erkannten fehlerhaften Sektoren im PGP Universal Server aufgezeichnet und der Verschlüsselungsvorgang wird fortgesetzt.

Viele Festplatten weisen fehlerhafte Sektoren auf. Falls PGP Whole Disk Encryption während der Verschlüsselung fehlerhafte Sektoren erkennt, wird die Verschlüsselung angehalten. Es wird eine Warnung ausgegeben, dass von PGP Whole Disk Encryption Laufwerksfehler erkannt wurden. (Beachten Sie, dass diese Fehler nicht mit der Verschlüsselung zusammenhängen. Sie weisen lediglich darauf hin, dass die Festplatte gewartet werden muss.)

Sie haben folgende Möglichkeiten:

- Erzwingen Sie die Fortsetzung der Verschlüsselung, indem Sie auf **Ja** klicken. Laufwerksfehler treten häufig auf und sind oft harmlos. Durch Klicken auf **Ja** wird der Verschlüsselungsvorgang fortgesetzt und PGP Whole Disk Encryption ignoriert weitere Fehler.

- Halten Sie die Verschlüsselung an, indem Sie auf **Nein** klicken und entschlüsseln Sie die Festplatte vollständig. Reparieren Sie anschließend die Laufwerksfehler mit einem Tool , bevor Sie erneut versuchen, die Festplatte zu verschlüsseln. Wenn es Anzeichen dafür gibt, dass die Festplatte stark fragmentiert ist oder viele Sektoren fehlerhaft sind, sollten Sie unverzüglich die erforderliche Wartung durchführen, bevor Sie die Festplatte verschlüsseln.

Mit PGP Whole Disk Encryption verschlüsselte Laufwerke verwenden

Wenn Sie das Startlaufwerk (oder eine sekundäre Festplatte) des Systems mit PGP Whole Disk Encryption schützen, ändert sich das Verhalten beim Systemstart. Nach dem Einschalten wird zunächst der PGP BootGuard-Anmeldebildschirm angezeigt, in dem Sie zur Eingabe der Passphrase aufgefordert werden. Wenn Sie erfolgreich eine gültige Passphrase eingeben, entschlüsselt PGP Whole Disk Encryption das Laufwerk.

Wenn Sie ein mit PGP Whole Disk Encryption verschlüsseltes Laufwerk verwenden, wird es automatisch bei Bedarf entschlüsselt und geöffnet. Nachdem ein Laufwerk vollständig verschlüsselt wurde, ist auf den meisten neueren Computern keine merkliche Geschwindigkeitseinbuße festzustellen.

Nachdem Sie ein Laufwerk entsperrt haben, stehen die darauf befindlichen Dateien nicht nur Ihnen, sondern allen Personen zur Verfügung, die physischen Zugang zu dem System haben. Die Dateien bleiben so lange entsperrt, bis Sie den Computer herunterfahren und die Dateien dadurch wieder sperren.

Warnung: Da die Dateien so lange entsperrt bleiben, bis Sie sie wieder sperren, sollten Sie die Verwendung eines PGP Virtual Disk-Laufwerks für Dateien in Betracht ziehen, die gesichert sein müssen, während der Computer verwendet wird. Weitere Informationen finden Sie unter *PGP Virtual Disk-Laufwerke verwenden* (auf Seite 181).

Wenn Sie ein System mit einem verschlüsselten Startlaufwerk herunterfahren oder neu starten oder einen verschlüsselten Wechseldatenträger vom System entfernen, bleiben alle Dateien auf dem Laufwerk verschlüsselt und vollständig geschützt. Daten werden niemals in einem nicht verschlüsselten Format auf das Laufwerk geschrieben. Damit Sie wieder auf die Dateien zugreifen können, ist die korrekte Authentifizierung (Passphrase oder privater Schlüssel) erforderlich.

Authentifizierung im PGP BootGuard-Bildschirm

Es gibt zwei mögliche Gründe dafür, dass Sie im PGP BootGuard-Anmeldebildschirm zur Eingabe der richtigen Passphrase für das geschützte Laufwerk aufgefordert werden:

- Wenn das Startlaufwerk mit PGP Whole Disk Encryption geschützt ist, müssen Sie sich ordnungsgemäß authentifizieren, damit der Systemstart erfolgen kann. Dies ist erforderlich, da die Betriebssystemdateien, die den Systemstart steuern, verschlüsselt sind und entschlüsselt werden müssen, bevor sie zum Starten des Systems verwendet werden können.
- Wenn eine sekundäre Festplatte mit PGP Whole Disk Encryption geschützt ist, können Sie sich beim Systemstart authentifizieren. Es ist dann keine Authentifizierung mehr erforderlich, wenn Sie später auf Dateien auf der sekundären Festplatte zugreifen möchten. Da die Dateien auf der sekundären Festplatte (die nicht zum Starten verwendet wird) für den Systemstart nicht erforderlich sind, werden Sie beim Systemstart nicht zur Authentifizierung aufgefordert. Mit der Funktion „Umgehen“ können Sie die Authentifizierung beim Systemstart überspringen. Sie werden dann später zur Authentifizierung aufgefordert, wenn Sie Dateien auf der sekundären Festplatte verwenden möchten.

Hinweis: Im PGP BootGuard-Anmeldebildschirm werden die Authentifizierungsdaten aller Benutzer akzeptiert, die für ein verschlüsseltes Laufwerk konfiguriert sind. Wenn beispielsweise auf einem System zwei Benutzer für ein Startlaufwerk und zwei weitere Benutzer für eine sekundäre Festplatte konfiguriert sind, kann sich *jeder* dieser vier konfigurierten Benutzer beim Systemstart mit seiner Passphrase im PGP BootGuard-Anmeldebildschirm authentifizieren. Dies umfasst auch die zwei Benutzer, die auf der sekundären Festplatte konfiguriert sind.

Im PGP BootGuard-Anmeldebildschirm können Sie ein verschlüsseltes Startlaufwerk oder ein sekundäres Laufwerk im System authentifizieren.

So authentifizieren Sie sich im PGP BootGuard-Anmeldebildschirm

1 Führen Sie einen Start oder Neustart des Systems aus, auf dem ein Laufwerk mit PGP Whole Disk Encryption verschlüsselt ist. Beim Systemstart wird der PGP BootGuard-Anmeldebildschirm angezeigt.

2 Geben Sie eine gültige Passphrase ein und drücken Sie die **Eingabetaste**.

Hinweis: Einige Zeichen können im PGP BootGuard-Bildschirm nicht eingegeben werden. Weitere Informationen finden Sie unter *Unterstützte Zeichen* (auf Seite 159).

Damit die Zeichen bei der Eingabe angezeigt werden, drücken Sie vor der Eingabe die **Tabulatortaste**.

Falls Sie sich bei der Eingabe verschreiben oder möglicherweise verschrieben haben, drücken Sie die Taste **Esc**, um alle Zeichen zu löschen und die Eingabe zu wiederholen.

3 Wenn Sie eine gültige Passphrase eingegeben haben, wird der PGP BootGuard-Anmeldebildschirm ausgeblendet und das System wird normal gestartet.

Wenn Sie eine ungültige Passphrase eingegeben haben, wird eine Fehlermeldung angezeigt. Geben Sie die Passphrase in diesem Fall erneut ein.

Schutz von Laufwerken aufrechterhalten

In den folgenden Abschnitten wird das Arbeiten mit Laufwerken beschrieben, die mit PGP Whole Disk Encryption verschlüsselt wurden.

Schlüsselinformationen auf verschlüsselten Laufwerken anzeigen

▸ **So zeigen Sie Schlüsselinformationen eines Benutzers öffentlicher Schlüssel auf einem verschlüsselten Laufwerk an**

1. Wählen Sie das verschlüsselte Laufwerk mit dem Benutzer öffentlicher Schlüssel aus, dessen Schlüsselinformationen Sie anzeigen möchten.
2. Klicken Sie in der Liste **Benutzerzugriff** bei gedrückter Ctrl-Taste oder bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste auf den Benutzernamen.
3. Klicken Sie im Kontextmenü auf **Schlüssel-Info anzeigen.** Der Bildschirm **Schlüssel-Info** für den ausgewählten Schlüssel wird angezeigt.

Systempartition ändern

Nehmen Sie an der Systempartition auf einem mit PGP Whole Disk Encryption verschlüsselten Startlaufwerk keine Änderungen vor, da sie andernfalls beim nächsten Systemstart fehlerhaft gestartet wird. Wenn die Partition eines verschlüsselten Laufwerks geändert werden muss, entschlüsseln Sie es zunächst und nehmen danach die Änderungen vor.

Andere Benutzer zu verschlüsselten Laufwerken hinzufügen

Der Benutzer, der ein verschlüsseltes Laufwerk erstellt, kann das Laufwerk anderen Benutzern zugänglich machen. Diese zusätzlichen Benutzer können dann mit ihrer eigenen eindeutigen Passphrase oder ihrem privaten Schlüssel auf das verschlüsselte Laufwerk zugreifen. Pro verschlüsseltem Laufwerk können Sie bis zu 120 Benutzer hinzufügen.

Achtung: Wenn mehrere Benutzer auf mit PGP Whole Disk Encryption geschützte Laufwerke zugreifen können, ist gewährleistet, dass der Zugriff im Fall eines Verlusts der Passphrase weiterhin möglich ist. Benutzer, die für verschlüsselte Laufwerke konfiguriert sind, können sich im Anmeldebildschirm von PGP Whole Disk Encryption authentifizieren und dann jedes geschützte Laufwerk im System entsperren.

▸ **So fügen Sie Laufwerken, die mit PGP Whole Disk Encryption geschützt sind, weitere Benutzer hinzu**

1. Wählen Sie das verschlüsselte Laufwerk aus, dem Sie weitere Benutzer hinzufügen möchten.
2. Klicken Sie auf das Plussymbol (**+**) unter der Liste **Benutzerzugriff**.

3 Wählen Sie in der angezeigten Liste die Option **Benutzer öffentlicher Schlüssel hinzufügen** oder **Passphrasenbenutzer hinzufügen aus.**

- Wenn Sie die Option **Benutzer öffentlicher Schlüssel hinzufügen** auswählen, werden Sie aufgefordert, den öffentlichen Schlüssel der Benutzer auszuwählen, die Sie hinzufügen möchten. Ziehen Sie die gewünschten Benutzer aus der Spalte **Schlüsselquelle** in die Spalte **Hinzuzufügende Schlüssel** und klicken Sie auf **OK**.
- Wenn Sie die Option **Passphrasenbenutzer hinzufügen** auswählen, werden Sie aufgefordert, einen Benutzernamen und eine Passphrase für den Benutzer einzugeben, den Sie hinzufügen möchten. Geben Sie in das Feld **Benutzername** einen Benutzernamen für den Benutzer ein.

  Geben Sie in das Feld **Passphrase für diesen Benutzer eingeben** eine Passphrase ein. Wiederholen Sie die Eingabe der Passphrase im Feld **Passphrase des Benutzers bestätigen**. Wenn die Zeichen während der Eingabe der Passphrase angezeigt werden sollen, wählen Sie **Tastatureingabe anzeigen** aus.

  Klicken Sie auf **OK**.

Sie werden zur Eingabe der Passphrase für das verschlüsselte Laufwerk aufgefordert.

4 Geben Sie die Passphrase für das verschlüsselte Laufwerk ein und klicken Sie auf **OK**. Die angegebenen Benutzer öffentlicher Schlüssel bzw. Passphrasenbenutzer werden hinzugefügt.

Hinweis: Die Verschlüsselung mit öffentlichen Schlüsseln zählt aus folgenden Gründen zu den sichersten Schutzmaßnahmen beim Hinzufügen von anderen Benutzern zu Laufwerken, die mit PGP Whole Disk Encryption verschlüsselt sind: (1) Passphrasen müssen neuen Benutzern nicht mitgeteilt werden. Das Risiko, dass Passphrasen von unberechtigten Personen abgefangen oder zufällig mitgehört werden, ist daher sehr gering. (2) Andere Benutzer müssen sich keine weiteren Passphrasen merken. (3) Die Verwaltung einer Liste von Benutzern wird vereinfacht, wenn jeder Benutzer einen eigenen privaten Schlüssel für den Zugriff auf das Laufwerk verwendet.

Benutzer von verschlüsselten Laufwerken löschen

Gelegentlich kann es erforderlich sein, einem Benutzer den Zugriff auf ein verschlüsseltes Laufwerk zu entziehen.

So entfernen Sie einen Benutzer von einem verschlüsselten Laufwerk

1 Wählen Sie das verschlüsselte Laufwerk aus, von dem Sie einen Benutzer entfernen möchten.

2 Wählen Sie in der Liste **Benutzerzugriff** den Namen des Benutzers aus, den Sie entfernen möchten.

3 Klicken Sie auf das Minussymbol (–) unter der Liste **Benutzerzugriff**. Sie werden zur Eingabe der Passphrase für das verschlüsselte Laufwerk aufgefordert.

4 Geben Sie die Passphrase für das verschlüsselte Laufwerk ein und klicken Sie auf **OK**. Der andere Benutzer wird entfernt.

Hinweis: Es ist nicht möglich, alle Benutzer von einem verschlüsselten Laufwerk zu entfernen. Wenn nur noch ein Benutzer in der Benutzerzugriffsliste aufgeführt ist, kann dieser Benutzer nicht entfernt werden.

Benutzer-Passphrasen ändern

▸ **So ändern Sie die Passphrase eines Passphrasenbenutzers auf einem verschlüsselten Laufwerk**

1 Wählen Sie das verschlüsselte Laufwerk mit dem Benutzer aus, dessen Passphrase geändert werden soll.

2 Klicken Sie in der Liste **Benutzerzugriff** bei gedrückter Ctrl-Taste oder bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste auf den Benutzernamen.

3 Wählen Sie aus dem Kontextmenü die Option **Benutzerpassphrase ändern aus.** Sie werden zur Eingabe der Passphrase für das verschlüsselte Laufwerk aufgefordert.

4 Geben Sie die Passphrase für das verschlüsselte Laufwerk ein und klicken Sie auf **OK**. Der Bildschirm **PGP-Passphrase bestätigen** wird angezeigt.

5 Geben Sie im Feld **Neue Passphrase eingeben** eine neue Passphrase ein, wechseln Sie zum Feld **Bestätigen und geben Sie die neue Passphrase erneut ein. Klicken Sie auf OK**.

6 Klicken Sie im Dialogfeld „Passphrase geändert“ auf **OK**. Die Passphrase wird geändert.

Verschlüsselte Laufwerke umschlüsseln

Ziehen Sie die Umschlüsselung von geschützten Laufwerken bzw. Partitionen in Betracht, wenn eine Passphrase eventuell in die falschen Hände geraten ist.

PGP Whole Disk Encryption verwendet für die Umschlüsselung von Laufwerken zwar denselben Verschlüsselungsalgorithmus (AES-256), jedoch einen anderen zugrunde liegenden Verschlüsselungsschlüssel. Dieses Verfahren kann mit dem Entschlüsseln und erneuten Verschlüsseln von Laufwerken verglichen werden, jedoch ist der Vorgang wesentlich schneller.

So schlüsseln Sie ein verschlüsseltes Laufwerk um

1. Wählen Sie das verschlüsselte Laufwerk aus, das umgeschlüsselt werden soll.
2. Klicken Sie im Menü **Laufwerk** auf **Laufwerk umschlüsseln**. Sie werden zur Eingabe der Passphrase für das verschlüsselte Laufwerk aufgefordert.
3. Geben Sie die Passphrase für das verschlüsselte Laufwerk ein und klicken Sie auf **OK**. Der Umschlüsselungsvorgang wird gestartet.

Sicherungskopien erstellen und Daten wiederherstellen

Während die meisten Sicherungsprogramme die Daten auf einem mit PGP Whole Disk Encryption verschlüsselten Laufwerk sichern können, treten bei einigen Sicherungsprogrammen Probleme auf. Bei diesen Sicherungsprogrammen kommt es zu Problemen, wenn die Datei „PGPWDE01“ auftritt (eine von PGP Whole Disk Encryption verwendete Datei). Als Lösung können Sie bei diesen Programmen die Datei „PGPWDE01“ von der Sicherung ausschließen (bei den meisten Sicherungsprogrammen ist der Ausschluss einzelner Dateien möglich). Wenn Sie eine Sicherungskopie mit diesen Programmen erstellt haben, sollten Sie prüfen, ob diese Sicherungskopie funktioniert.

Automatische Sicherungssoftware auf einem mit PGP Whole Disk Encryption verschlüsselten Laufwerk verwenden

Sie können Laufwerke, die mit PGP Whole Disk Encryption geschützt sind, automatisch sichern. Von der Software gesicherte Dateien werden vor dem Erstellen der Sicherungskopie entschlüsselt.

Beispielsweise werden Sicherungskopien mit Time Machine, der automatischen Sicherungssoftware von Mac OS X 10.5 (Leopard), normal erstellt und die Dateien der Sicherungskopie sind nicht verschlüsselt.

Hinweis: Software für die Datenwiederherstellung (z. B. die Mac OS X-Version von Boomerang Data Recovery) versucht, Daten von einer Festplatte wiederherzustellen, auf die derzeit nicht zugegriffen werden kann. Wird Software für die Datenwiederherstellung für eine Festplatte verwendet, die mit PGP Whole Disk Encryption geschützt ist, liegen die verschlüsselten Daten *nicht* in einem verwendbaren Format vor.

PGP Desktop von verschlüsselten Laufwerken deinstallieren

Wenn auf einem System Laufwerke mit PGP Whole Disk Encryption geschützt sind und PGP Desktop deinstalliert wird, ist der Zugriff auf diese Laufwerke nicht mehr möglich. Aus diesem Grund wird durch eine Sicherheitsfunktion die Deinstallation von PGP Desktop verhindert, wenn auf dem System Laufwerke mit PGP Whole Disk Encryption geschützt sind. In diesem Fall wird eine Fehlermeldung angezeigt, dass die Deinstallation abgebrochen wird, um die verschlüsselten Laufwerke zu schützen.

Wenn Sie PGP Desktop deinstallieren möchten, entschlüsseln Sie zunächst alle mit PGP Whole Disk Encryption geschützten Laufwerke.

PGP Whole Disk Encryption in einer von einem PGP Universal Server verwalteten Umgebung verwenden

PGP Whole Disk Encryption kann für Benutzer von PGP Desktop verwaltet werden, die in einer von einem PGP Universal Server verwalteten Umgebung arbeiten. Administratoren können Benutzern in ihrem Unternehmen Installationsprogramme für PGP Desktop bereitstellen.

PGP Whole Disk Encryption verwalten

Der PGP-Administrator kann Folgendes steuern:

- **Die Verfügbarkeit der PGP Whole Disk Encryption-Funktion für Benutzer**. Wenn Sie in einer von PGP Universal verwalteten Umgebung arbeiten und die PGP Whole Disk Encryption-Funktion *nicht* verfügbar ist, erkundigen Sie sich beim PGP-Administrator, ob die Funktion durch eine Richtlinie deaktiviert wurde.

  Für die PGP Whole Disk Encryption-Funktion ist außerdem eine entsprechende Lizenz von der PGP Corporation erforderlich. Wenn die Funktion für Sie deaktiviert ist, obwohl sie durch eine Richtlinien aktiviert wurde, wenden Sie sich an den PGP-Administrator, um sicherzustellen, dass Sie über eine entsprechende Lizenz verfügen.

- **Die Möglichkeit der Wiederherstellung von Laufwerken, die mit PGP Whole Disk Encryption geschützt sind**. Wenn Sie die Passphrase für ein mit PGP Whole Disk Encryption verschlüsseltes Laufwerk vergessen ist das Laufwerk nicht zugänglich. Wenn Sie die PGP Whole Disk Encryption-Funktion jedoch in einer von einem PGP Universal Server verwalteten Umgebung verwenden, erkundigen Sie sich beim PGP-Administrator, ob eine Laufwerkswiederherstellung möglich ist.

- **Die Notwendigkeit der Verschlüsselung des Startlaufwerks mit PGP Whole Disk Encryption bei der Installation von PGP Desktop**.

Wenn Sie mit PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung arbeiten, erhalten Sie weitere Informationen vom PGP-Administrator.

Wenn sich Ihre Richtlinien ändern sollten, insbesondere von der Möglichkeit zur Verschlüsselung eines Laufwerks zur Deaktivierung dieser Funktion, können Sie alle bereits mit Whole Disk Encryption verschlüsselten Laufwerke trotzdem weiterhin verwenden. Jedoch können Sie keine weiteren Laufwerke mehr verschlüsseln, bestehende verschlüsselte Laufwerke umschlüsseln oder neue Benutzer hinzufügen.

Wiederherstellungs-Token erstellen

Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten und Sie entsprechend der für Sie geltenden Richtlinien Wiederherstellungs-Token für das gesamte Laufwerk erstellen können, wird von PGP Desktop immer dann ein Wiederherstellungs-Token erstellt, wenn Sie ein Laufwerk, eine Partition (unter Windows) oder einen Wechseldatenträger mit PGP Whole Disk Encryption verschlüsseln. Dieses Wiederherstellungs-Token kann zum Zugriff auf das Laufwerk oder die Partition (unter Windows) verwendet werden, falls die Passphrase oder das Authentifizierungs-Token (unter Windows) verloren gegangen ist.

Falls die für Sie geltenden Richtlinien diese Funktion nicht unterstützen oder falls Sie nicht in einer von einem PGP Universal Server verwalteten Umgebung mit einer vorkonfigurierten Installation von PGP Desktop arbeiten, können Sie keine Whole Disk-Wiederherstellungs-Token verwenden.

Dieses Wiederherstellungs-Token wird automatisch an den PGP Universal Server gesendet, der für die Verwaltung der Sicherheit des mit PGP Whole Disk Encryption geschützten Laufwerks bzw. der Partition (unter Windows) zuständig ist.

Wenn Sie in einer von einem PGP Universal Server verwalteten Umgebung arbeiten und die Passphrase oder das Authentifizierungs-Token für den Schutz eines Laufwerks oder einer Partition (unter Windows) mit PGP Whole Disk Encryption verlieren, bitten Sie den PGP-Administrator, Sie bei der Verwendung des Wiederherstellungs-Tokens zu unterstützen.

Das Wiederherstellungs-Token kann nur einmal verwendet werden, um auf ein Laufwerk oder eine Partition (unter Windows) zuzugreifen, das bzw. die mit PGP Whole Disk Encryption geschützt ist. Sobald ein Wiederherstellungs-Token verwendet wurde, wird automatisch ein neues Token erstellt und an den PGP Universal Server gesendet. Der Benutzer von PGP Desktop erhält die Möglichkeit, einen neuen Benutzer zu erstellen oder die auf dem Laufwerk bzw. der Partition vorhandenen Benutzer beizubehalten.

Beachten Sie, dass das Wiederherstellungs-Token nur verwendet wird, um auf ein verschlüsseltes Laufwerk oder eine verschlüsselte Partition (unter Windows) zuzugreifen. Das Wiederherstellungs-Token kann nicht zur Verschlüsselung oder Entschlüsselung von Daten genutzt werden.

Achtung: Wenn die Sicherheit der mit PGP Whole Disk Encryption verschlüsselten Laufwerke bzw. Partitionen (unter Windows) durch den Verlust oder die Offenlegung der Passphrase oder des Authentifizierungs-Tokens (unter Windows) beeinträchtigt ist, sollten Sie die Umschlüsselung der Laufwerke bzw. Partitionen in Betracht ziehen. Hierbei wird das Laufwerk oder die Partition mit demselben Verschlüsselungsalgorithmus umgeschlüsselt, jedoch wird ein anderer zugrunde liegender Verschlüsselungsschlüssel verwendet. Dieses Verfahren kann mit dem Entschlüsseln und erneuten Verschlüsseln von Laufwerken bzw. Partitionen verglichen werden, jedoch ist der Vorgang wesentlich schneller.

Wiederherstellungs-Token verwenden

Nachdem Sie ein Wiederherstellungs-Token vom PGP Universal-Administrator erhalten haben, führen Sie die folgenden Schritte aus, um das Laufwerk zu entsperren.

Bei der Eingabe des Wiederherstellungs-Tokens müssen Sie die Schreibweise in Bezug auf Groß-/Kleinschreibung (alles Großbuchstaben) oder Gedankenstriche, die Sie vom PGP Universal-Administrator erhalten haben, nicht einhalten. Sie können auf Wunsch nur Kleinbuchstaben ohne Gedankenstriche eingeben.

So verwenden Sie ein Wiederherstellungs-Token auf einem Startlaufwerk

- Geben Sie im PGP BootGuard-Bildschirm das Wiederherstellungs-Token in das Passphrasenfeld ein.

So verwenden Sie ein Wiederherstellungs-Token auf einem Wechseldatenträger

- Legen Sie das Laufwerk ein. Wenn Sie zur Eingabe der Passphrase aufgefordert werden, geben Sie das Wiederherstellungs-Token ein.

Daten von verschlüsselten Laufwerken wiederherstellen

In seltenen Fällen müssen Sie möglicherweise Daten von einem verschlüsselten Laufwerk wiederherstellen, das beschädigt oder zerstört wurde. Es kann auch vorkommen, dass Sie nicht über die Anmeldeinformationen zum Zugriff auf das Laufwerk verfügen (z. B. wenn das Laufwerk von einem ehemaligen Mitarbeiter verschlüsselt wurde).

In diesen Fällen haben Sie mehrere Möglichkeiten:

1 Verwenden Sie einen Wiederherstellungsdatenträger. Wenn vor der Verschlüsselung des Laufwerks oder der Partition ein Wiederherstellungsdatenträger erstellt wurde, kann dieser zur Entschlüsselung des Laufwerks verwendet werden. Weitere Informationen finden Sie unter *Wiederherstellungsdatenträger erstellen und verwenden* (auf Seite 173).

2 Verwenden Sie ein anderes System, um das Laufwerk zu entschlüsseln. Weitere Informationen zum Erstellen neuer Richtlinien oder zum Bearbeiten bestehender Richtlinien finden Sie unter *Mit PGP Whole Disk Encryption verschlüsselte Laufwerke entschlüsseln* (auf Seite 174).

3 Verwenden Sie das Whole Disk-Wiederherstellungs-Token. Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, wird das Wiederherstellungs-Token bei der Verschlüsselung des Laufwerks automatisch erstellt. Weitere Informationen finden Sie unter *Wiederherstellungs-Token verwenden* (auf Seite 172).

Weitere Informationen zum Wiederherstellen von Daten finden Sie im *PGP-Wissensdatenbankartikel 1018 https://support.pgp.com/?faq=1018*.

Weitere Informationen zum Wiederherstellen von Daten mithilfe des Target Disk Mode finden Sie im *PGP-Wissensdatenbankartikel 1583* (*http://support.pgp.com/?faq=1583*).

Wiederherstellungsdatenträger erstellen und verwenden

Obwohl die Wahrscheinlichkeit äußerst gering ist, dass eine boot.efi-Datei auf einem mit PGP Whole Disk Encryption verschlüsselten Startlaufwerk bzw. einer Startpartition beschädigt wird, kann dies nicht ausgeschlossen werden. In diesem Fall kann das System möglicherweise nicht gestartet werden. Damit Sie auf eine solche (unwahrscheinliche) Eventualität vorbereitet sind, sollten Sie eine Wiederherstellungs-CD erstellen, bevor Sie ein Startlaufwerk oder eine Startpartition mit PGP Desktop verschlüsseln.

Achtung: Beachten Sie, dass Wiederherstellungsdatenträger nur mit der Version von PGP Desktop kompatibel sind, mit der sie erstellt wurden. Wenn Sie beispielsweise versuchen, mit einem in Version 10.0.0 erstellten Wiederherstellungsdatenträger ein mit PGP Whole Disk Encryption Version 10.1 geschütztes Laufwerk zu entschlüsseln, kann nicht mehr auf das mit PGP Whole Disk Encryption Version 10.1 verschlüsselte Laufwerk zugegriffen werden.

Dieser Abschnitt enthält Verfahren zum Erstellen einer Wiederherstellungs-CD sowie Informationen zu ihrer Verwendung. Weitere Informationen finden Sie im *PGP-Wissensdatenbankartikel 1658* (*http://support.pgp.com/?faq=1658*).

So erstellen Sie eine Wiederherstellungs-CD

1 Laden Sie das ISO-Image für die Wiederherstellung auf das System herunter und speichern Sie es.

2 Brennen Sie das Image mit dem Mac OS X-Festplattendienstprogramm auf eine CD-ROM. Informationen hierzu finden Sie im *Artikel des Apple-Supports HT2087* (*http://support.apple.com/kb/HT2087*).

3 Nehmen Sie die Wiederherstellungs-CD aus dem Laufwerk und beschriften Sie sie entsprechend.

So verwenden Sie eine Wiederherstellungs-CD oder -diskette

Achtung: Wenn Sie mit der Entschlüsselung eines Laufwerks oder einer Partition mit einer Wiederherstellungs-CD oder -diskette begonnen haben, halten Sie den Vorgang nicht an. Abhängig von der Größe des zu entschlüsselnden Laufwerks kann dieser Vorgang einige Zeit dauern. Sie können das Laufwerk schneller entschlüsseln, indem Sie ein anderes System verwenden, auf dem dieselbe Version von PGP Desktop installiert ist. Weitere Informationen finden Sie unter *Mit PGP Whole Disk Encryption verschlüsselte Laufwerke entschlüsseln* (auf Seite 174).

1 Starten Sie das Macintosh-System mit der CD. Halten Sie dazu beim Starten des Systems die Wahltaste gedrückt und wählen Sie die Option für den Systemstart von der Wiederherstellungs-CD aus. Der PGP BootGuard-Bildschirm wird angezeigt.

2 Entschlüsseln Sie das Laufwerk, indem Sie die Taste D und dann die Eingabetaste drücken.

3 Geben Sie bei der Aufforderung die Passphrase ein und drücken Sie die Eingabetaste.

Mit PGP Whole Disk Encryption verschlüsselte Laufwerke entschlüsseln

Wenn Sie auf einem Laufwerk, das mit PGP Whole Disk Encryption geschützt ist, Aktivitäten zur Laufwerkswiederherstellung durchführen müssen, empfiehlt die PGP Corporation die vorherige Entschlüsselung des Laufwerks. Sie haben folgende Möglichkeiten zum Entschlüsseln eines Laufwerks:

- Verwenden Sie in PGP Desktop die Option **Laufwerk > Entschlüsseln** (weitere Informationen zum Verwenden dieser Option zum Entschlüsseln eines Laufwerks finden Sie im folgenden Verfahren).
- Schließen Sie einen Wechseldatenträger an ein zweites System an und entschlüsseln Sie diesen über die PGP Desktop-Software auf diesem System. Wenn der Wechseldatenträger im FAT-Format formatiert wurde, können Sie ihn mit PGP Desktop für Windows oder für Mac OS X entschlüsseln. Wenn der Datenträger als HFS-Laufwerk formatiert wurde, müssen Sie PGP Desktop für Mac OS X verwenden.

Wenn das Laufwerk entschlüsselt ist, können Sie mit der Wiederherstellung fortfahren.

So entschlüsseln Sie ein Laufwerk mit PGP Desktop

1. Öffnen Sie PGP Desktop, klicken Sie mit der rechten Maustaste auf das Laufwerk, das Sie entschlüsseln möchten, und wählen Sie **Entschlüsseln** aus. Das Dialogfeld „PGP-Passphrase eingeben“ wird angezeigt.
2. Geben Sie die Passphrase zum Entsperren des Laufwerks ein und klicken Sie auf **OK**. Im Fenster von PGP Desktop wird eine Fortschrittsanzeige für die Entschlüsselung angezeigt.

   Auch die voraussichtliche Dauer zum Entschlüsseln des Laufwerks wird im Fenster von PGP Desktop angezeigt. Wenn Sie den Entschlüsselungsvorgang unterbrechen oder abbrechen möchten, klicken Sie auf **Anhalten**.

Wechseldatenträger auf anderen Systemen verwenden

Sie können Wechseldatenträger, die unter Windows formatiert wurden, auf andere Mac OS X-Systeme übertragen, auf denen PGP Desktop 10.1 installiert ist, und dann auf dem anderen System auf die verschlüsselten Dateien zugreifen.

Sie müssen sich für den Zugriff auf den Inhalt des Datenträgers authentifizieren können.

Hinweis: Sie benötigen zum Schützen eines Datenträgers mit PGP Whole Disk Encryption die entsprechende PGP Desktop-Lizenz. Wenn Sie jedoch einen mit Windows formatierten Wechseldatenträger mit PGP Whole Disk Encryption verschlüsselt haben, können Sie diesen Wechseldatenträger auf einem anderen Computer mit PGP Desktop 10.1 auch dann verwenden, wenn dieser Computer nicht über eine PGP Desktop-Lizenz für PGP Whole Disk Encryption verfügt.

Auf Daten auf verschlüsselten Wechseldatenträgern zugreifen

Wenn Sie einen Wechseldatenträger (z. B. ein USB-Flash-Laufwerk) mit PGP Whole Disk Encryption für Windows schützen, können Sie diesen Wechseldatenträger auf einem anderen Windows- oder Mac OS X-System verwenden und auf diesem anderen System auf die verschlüsselten Dateien auf dem Datenträger zugreifen. Auf mit PGP Whole Disk Encryption unter Linux erstellte Wechseldatenträger kann nur mit PGP Desktop Version 10.0 oder höher zugegriffen werden.

Sie müssen eine Authentifizierung durchführen, um auf den Inhalt des Datenträgers zuzugreifen.

Hinweis: Beachten Sie die PGP Desktop-Lizenzierung, wenn Sie einen verschlüsselten Wechseldatenträger auf einem anderen System verwenden. Sie benötigen zum Schützen eines Datenträgers mit PGP Whole Disk Encryption die entsprechende PGP Desktop-Lizenz. Wenn Sie jedoch einen Wechseldatenträger mit PGP Whole Disk Encryption verschlüsselt haben, können Sie diesen Wechseldatenträger auf einem anderen Computer mit PGP Desktop 9.5.2 oder höher auch dann verwenden, wenn dieser Computer nicht über eine PGP Desktop-Lizenz für PGP Whole Disk Encryption verfügt.

Spezielle Sicherheitsmaßnahmen von PGP Desktop

PGP Desktop verfügt über Funktionen, mit denen Sicherheitsprobleme mit PGP Whole Disk Encryption vermieden werden können. Diese Vorsichtsmaßnahmen gelten auch für PGP Virtual Disk-Laufwerke.

Löschung der Passphrase

Wenn Sie eine Passphrase eingeben, wird diese von PGP Desktop nur für kurze Zeit verwendet und danach aus dem Speicher gelöscht. PGP Desktop erstellt außerdem keine Kopien der Passphrase. Daher befindet sich die Passphrase in der Regel nur für den Bruchteil einer Sekunde im Speicher. Diese Funktion ist von größter Bedeutung, da sonst andere Personen im Hauptspeicher nach der Passphrase suchen könnten, während Sie nicht an Ihrem Arbeitsplatz sind. Diese Personen würden dann ohne Ihr Wissen vollständigen Zugriff auf alle mit dieser Passphrase geschützten Daten erhalten.

Schutz des virtuellen Speichers

Ihre Passphrase oder andere Schlüssel könnten mit den Daten des virtuellen Speichersystems auf die Festplatte ausgelagert werden. PGP Desktop lässt jedoch nicht zu, dass die Passphrasen und Schlüssel auf die Festplatte geschrieben werden. Mit dieser Funktion wird verhindert, dass unberechtigte Personen die virtuelle Speicherdatei nach Passphrasen durchsuchen.

Schutz durch MSIM (Memory Static Ion Migration)

Wenn Sie ein Laufwerk oder eine Partition (unter Windows) mit PGP Whole Disk Encryption schützen, wird Ihre Passphrase in einen Schlüssel umgewandelt. Dieser Schlüssel dient zum Verschlüsseln und Entschlüsseln der Daten auf dem verschlüsselten Laufwerk bzw. der verschlüsselten Partition. Obwohl die Passphrase sofort aus dem Speicher gelöscht wird, bleibt der Schlüssel (aus dem die Passphrase nicht abgeleitet werden kann) jedoch im Speicher erhalten.

Dieser Schlüssel wird zwar nicht im virtuellen Speicher gespeichert, wenn jedoch ein bestimmter Speicherbereich genau dieselben Daten für extrem lange Zeiträume speichert, ohne dass der Computer ausgeschaltet oder zurückgesetzt wird, bleibt eine statische Ladung im Speicher zurück, die von Angreifern gelesen werden könnte. Wenn Ihr verschlüsseltes Laufwerk bzw. Ihre verschlüsselte Partition (unter Windows) für einen langen Zeitraum entschlüsselt ist, können mit der Zeit erkennbare Spuren des Schlüssels im Speicher zurückbleiben. Mit bestimmten Geräten könnte der Schlüssel wiederhergestellt werden. Diese Geräte sind zwar nicht im Elektronikfachgeschäft um die Ecke zu finden, stehen wahrscheinlich jedoch größeren Regierungsbehörden zur Verfügung.

PGP Desktop schützt vor derartigen Angriffen, indem zwei Kopien (eine normale Kopie und eine Kopie mit umgekehrten Bit) im RAM-Speicher gehalten und alle paar Sekunden umgekehrt werden.

Weitere Sicherheitsaspekte

Im Allgemeinen hängt die Fähigkeit zum Schützen von Daten von den Vorkehrungen ab, die Sie treffen. Kein Verschlüsselungsprogramm kann Sie vor unzureichenden Sicherheitsmaßnahmen schützen. Wenn Sie sich z. B. vom Schreibtisch entfernen und dabei den Computer eingeschaltet und vertrauliche Dateien geöffnet lassen, kann jeder auf die Informationen zugreifen, auch wenn das Laufwerk oder die Partition (unter Windows) mit PGP Whole Disk Encryption geschützt ist.

Im Folgenden sind einige Empfehlungen zur Wahrung der optimalen Sicherheit aufgeführt:

- Verwenden Sie einen Bildschirmschoner mit Kennwortschutz, um anderen Personen den Zugriff auf Ihren Computer oder das Anzeigen Ihres Bildschirms zu erschweren, wenn Sie sich nicht an Ihrem Schreibtisch befinden.

- Stellen Sie sicher, dass die verschlüsselten Laufwerke oder Partitionen (unter Windows) nicht für andere Computer im Netzwerk freigegeben sind. Wenden Sie sich dazu ggf. an den Netzwerkadministrator. Wenn Sie Laufwerke oder Partitionen entsperrt haben, wird der Inhalt nicht mehr durch PGP Whole Disk Encryption geschützt. Sie können von allen Personen angezeigt werden, die im Netzwerk darauf zugreifen können. Verwenden Sie PGP Virtual Disk zum Speichern von Dateien, die auch gesperrt bleiben müssen, während Sie am Computer arbeiten.
- Schreiben Sie Ihre Passphrase auf keinen Fall auf. Wählen Sie eine Passphrase, die Sie sich merken können. Wenn Sie sich die Passphrase nur schwer merken können, verwenden Sie eine Gedächtnisstütze (z. B. Poster, Lieder, Gedichte oder Witze), jedoch *schreiben Sie die Passphrase nicht auf*.
- Wenn Sie PGP Desktop zu Hause einsetzen und den Computer gemeinsam mit anderen Personen nutzen, können diese wahrscheinlich Ihre geöffneten Dateien sehen, die sich auf mit PGP Whole Disk Encryption geschützten Laufwerken oder Partitionen (unter Windows) befinden. Solange Sie ein System mit durch PGP Whole Disk Encryption verschlüsselten Laufwerken oder Partitionen herunterfahren oder einen verschlüsselten Datenträger aus dem System entfernen, bleiben alle Dateien auf dem Laufwerk, der Partition bzw. dem Datenträger verschlüsselt und vollständig geschützt.
- Wenn Sie sich für längere Zeit vom Computer entfernen, empfiehlt Ihnen die PGP Corporation, das Macintosh-System herunterzufahren und nicht den Stromsparmodus zu verwenden. Dadurch wird sichergestellt, dass nach Aufheben des Stromsparmodus keine andere Person auf das verschlüsselte System zugreifen kann.

Technische Details zum Verschlüsseln von Startlaufwerken

Damit PGP Whole Disk Encryption für Startlaufwerke unter Mac OS X unterstützt wird, erstellt PGP Desktop eine neue Partition (mit der GUID-Partitionstabelle) und legt ein neues Startladeprogramm auf der neuen Partition ab.

Wichtig: In Versionen von PGP Desktop vor Version 10.1 wurden APM-Partitionen unterstützt. Diese Partitionierungsmethode unterstützt PGP Whole Disk Encryption für Startlaufwerke *nicht*, daher verwenden Version 9.9 und höher die GUID-Partitionstabelle (GPT). Aufgrund dieser Änderung müssen alle Laufwerke, die mit PGP Whole Disk mit älteren Versionen als PGP Desktop Version 9.9 verschlüsselt wurden, entschlüsselt werden, *bevor* Version 9.9 oder höher installiert wird. Auf ältere Laufwerke, die mit PGP Whole Disk verschlüsselt wurden und die vor der Installation von Version 9.9 nicht entschlüsselt werden, kann nach der Installation von Version 9.9 oder höher nicht mehr zugegriffen werden.

Das von PGP Desktop installierte Startladeprogramm führt Folgendes aus: Es authentifiziert Benutzer, die versuchen, das Laufwerk zu starten. Wenn die Authentifizierung erfolgreich ist, ruft das Programm das Mac OS X-Startladeprogramm auf und entschlüsselt die Dateien, die zum normalen Starten des Laufwerks erforderlich sind. Ist die Authentifizierung nicht erfolgreich, wird das Mac OS X-Startladeprogramm nicht aufgerufen und die erforderlichen Dateien werden nicht entschlüsselt, sodass das Laufwerk nicht gestartet wird.

Achtung: Boot Camp von Apple funktioniert nur, wenn das Laufwerk zwei Partitionen aufweist: eine für Mac OS X und eine für Boot Camp. Da PGP Desktop eine weitere Partition hinzufügt, funktioniert Boot Camp nicht auf einem Mac OS X-System mit PGP Desktop 10.1 oder höher. Andere Visualisierungssoftware (z. B. Parallels) funktioniert ordnungsgemäß auf einem Mac OS X-System mit PGP Desktop 10.1 oder höher. Die PGP Corporation empfiehlt eindringlich, Apple Boot Camp vor der Installation von PGP Desktop zu deinstallieren.

12 PGP Virtual Disk-Laufwerke verwenden

Sie können mit PGP Virtual Disk-Laufwerken Ihre Dateien organisieren, Dateien mit ähnlichen Namen getrennt speichern oder mehrere Versionen derselben Dokumente und Programme separat verwalten.

In diesem Abschnitt wird die PGP Virtual Disk-Funktion von PGP Desktop beschrieben.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat der PGP Universal Server-Administrator möglicherweise bestimmte Funktionen deaktiviert. Wenn eine Funktion deaktiviert wurde, wird das entsprechende Bedienelement auf der linken Seite nicht angezeigt und das Menü und andere Optionen für diese Funktion sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn der PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Informationen zu PGP Virtual Disk-Laufwerken 182
Neue PGP Virtual Disk-Laufwerke erstellen 183
Eigenschaften von PGP Virtual Disk-Laufwerken anzeigen 186
Aktivierte PGP Virtual Disk-Laufwerke verwenden 187
Mit anderen Benutzern arbeiten 190
Benutzer-Passphrasen ändern 194
PGP Virtual Disk-Laufwerke löschen 195
PGP Virtual Disk-Laufwerke warten 195
PGP Virtual Disk-Verschlüsselungsalgorithmen 198
Spezielle Sicherheitsfunktionen von PGP Virtual Disk 199

Hinweis: In früheren Versionen von PGP Desktop wurden PGP Virtual Disk-Laufwerke als *PGP Disk*-Laufwerke bezeichnet. Die Bezeichnung *PGP Disk* umfasst jetzt sowohl die Funktionen PGP Virtual Disk als auch PGP Whole Disk Encryption.

Informationen zu PGP Virtual Disk-Laufwerken

Ein PGP Virtual Disk-Laufwerk ist ein Speicherplatzbereich auf einem mit dem Computer verbundenen Datenträger. Dieser Speicherplatzbereich wird verschlüsselt und separat verwaltet. PGP Virtual Disk-Laufwerke sind mit einem Banktresor vergleichbar und eignen sich hervorragend für den Schutz vertraulicher Dateien, während der Rest des Computers unverschlüsselt zur Verfügung steht.

Die Funktionsweise eines PGP Virtual Disk-Laufwerks ist mit der eines zusätzlichen Festplattenlaufwerks zu vergleichen, obwohl es sich eigentlich um eine einzelne Datei handelt, die sich auf einer beliebigen Festplatte des Computers befinden kann. Die Datei bietet Speicherplatz für Dateien jeden Typs. Auf einem PGP Virtual Disk-Laufwerk können Sie sogar Anwendungen installieren oder Dateien speichern. Das Besondere daran ist jedoch, dass sich ein solches Laufwerk jederzeit und ohne Auswirkungen auf den Rest des Computers sperren lässt. Wenn Sie die auf einem PGP Virtual Disk-Laufwerk gespeicherten Anwendungen oder Dateien verwenden möchten, entsperren Sie das Laufwerk. Dadurch können Sie wieder auf die Dateien zugreifen.

PGP Virtual Disk-Laufwerke werden entsperrt und gesperrt, indem sie auf dem Computer aktiviert bzw. deaktiviert werden. PGP Desktop unterstützt Sie bei diesem Vorgang.

Die Größe eines PGP Virtual Disk-Laufwerks kann festgelegt werden, jedoch ist auch die Erstellung eines dynamisch dimensionierten Laufwerks möglich, dessen Kapazität bei Bedarf erweitert wird. Die Größe, die Sie bei der Erstellung des Laufwerks vorgeben, bezeichnet die maximale Größe des Laufwerks.

Nach der Aktivierung eines PGP Virtual Disk-Laufwerks sind folgende Aktionen möglich:

- Verschieben oder Kopieren von Dateien auf das aktivierte PGP Virtual Disk-Laufwerk bzw. von diesem Laufwerk
- Speichern von Dateien auf dem aktivierten PGP Virtual Disk-Laufwerk
- Installieren von Anwendungen auf dem PGP Virtual Disk-Laufwerk

Dateien und Anwendungen auf einem PGP Virtual Disk-Laufwerk werden verschlüsselt gespeichert. Falls der Computer während der Deaktivierung eines PGP Virtual Disk-Laufwerks abstürzt, bleibt der Inhalt des Laufwerks sicher verschlüsselt.

Deaktivierte PGP Virtual Disk-Laufwerke werden nicht in Windows Explorer oder im Finder von Mac OS X aufgeführt und sind für Benutzer ohne korrekte Authentifizierung nicht zugänglich.

Beachten Sie, dass die Daten in der verschlüsselten Datei sicher gespeichert bleiben und nur entschlüsselt werden, wenn Sie auf eine der Dateien zugreifen. Durch diese Art der Datenspeicherung können PGP Virtual Disk-Laufwerke problemlos bearbeitet und mit anderen Personen ausgetauscht werden, jedoch gehen die Daten verloren, wenn die Laufwerksdatei gelöscht wird. Es ist daher ratsam, Sicherungskopien der verschlüsselten Dateien zu erstellen, damit die Daten im Notfall wiederhergestellt werden können.

Informationen zu PGP-Optionen für PGP Virtual Disk-Laufwerke finden Sie unter *Laufwerksoptionen* (siehe "*Laufwerkseinstellungen*" auf Seite 228).

Achtung: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, müssen Sie nach der Installation von PGP Desktop möglicherweise ein PGP Virtual Disk-Laufwerk erstellen. In diesem Fall wurden Größe, Dateisystem und Algorithmus u. U. festgelegt. Weitere Informationen finden Sie unter *PGP Desktop mit PGP Universal Server verwenden* (auf Seite 239).

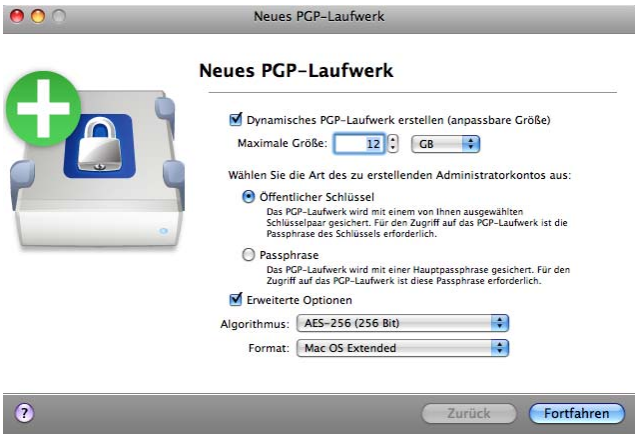
Neue PGP Virtual Disk-Laufwerke erstellen

So erstellen Sie ein neues PGP Virtual Disk-Laufwerk

1 Öffnen Sie PGP Desktop und klicken Sie auf **PGP Disk**. Das Fenster **PGP Disk** wird angezeigt.

Hinweis: Wenn Sie PGP Whole Disk nicht mit der entsprechenden Lizenz installiert haben, wird in diesem Fenster nur die Option „Neues Volumen“ angezeigt. (Die Installationsoption „PGP Whole Disk“ stand während der Installation von PGP Desktop unter **Benutzerdefiniert** zur Verfügung.)

2 Klicken Sie auf **Neues PGP Virtual Disk-Laufwerk**. Der Bildschirm „Neues PGP-Laufwerk“ wird angezeigt.


Neues PGP-Laufwerk
Neues PGP-Laufwerk
Dynamisches PGP-Laufwerk erstellen (anpassbare Größe)
Maximale Größe:
12
GB
Wählen Sie die Art des zu erstellenden Administratorkontos aus:
Öffentlicher Schlüssel
Das PGP-Laufwerk wird mit einem von Ihnen ausgewählten Schlüsselpaar gesichert. Für den Zugriff auf das PGP-Laufwerk ist die Passphrase des Schlüssels erforderlich.
Passphrase
Das PGP-Laufwerk wird mit einer Hauptpassphrase gesichert. Für den Zugriff auf das PGP-Laufwerk ist diese Passphrase erforderlich.
Erweiterte Optionen
Algorithmus:
AES-256 (256 Bit)
Format:
Mac OS Extended
Zurück
Fortfahren

3 Geben Sie in das Feld für die Eingabe der gewünschten Größe für das PGP-Laufwerk **die Größe des neuen PGP Virtual Disk-Laufwerks ein. Geben Sie ganze Zahlen ohne Dezimalstellen ein. Sie können den im Feld angezeigten Wert auch mit den Pfeilen erhöhen bzw. verringern. Wählen Sie im Menü die Einheit KB (Kilobyte), MB (Megabyte) oder GB (Gigabyte) aus.**

4 Wählen Sie den Authentifizierungstyp aus, der für den primären Benutzer des PGP Virtual Disk-Laufwerks verwendet werden soll:

- Wenn Sie das PGP Virtual Disk-Laufwerk mit Ihrem Schlüsselpaar schützen möchten, wählen Sie **Öffentlicher Schlüssel** aus.
- Wenn Sie das PGP Virtual Disk-Laufwerk mit einer Passphrase schützen möchten, wählen Sie **Passphrasenbenutzer** aus.

5 Wenn Sie die erweiterten Optionen anzeigen oder ändern möchten, aktivieren Sie das Kontrollkästchen **Erweiterte Optionen**. Das Kontrollkästchen **Größe des PGP Virtual Disk-Laufwerks bei Bedarf automatisch anpassen** sowie die Menüs **Algorithmus** und **Format** werden angezeigt.

Achtung: Die Standardeinstellungen für **Erweiterte Optionen** sind für die meisten Benutzer geeignet. Ändern Sie diese Einstellungen nur, wenn Sie mit ihnen vertraut sind.

- Aktivieren Sie das Kontrollkästchen **Größe des PGP Virtual Disk-Laufwerks bei Bedarf automatisch anpassen**, wenn PGP Desktop die Größe des neuen **PGP Virtual Disk-Laufwerks automatisch verwalten soll. Die Laufwerksgröße wird dann beim Hinzufügen oder Löschen von Dateien entsprechend geändert.**

Achtung: Die Option **Größe des PGP Virtual Disk-Laufwerks bei Bedarf automatisch anpassen** kann nur beim Erstellen eines PGP Virtual Disk-Laufwerks festgelegt werden. Wenn das PGP Virtual Disk-Laufwerk erstellt ist, können Sie nicht mehr zwischen fester Größe und automatischer Größenanpassung wechseln.

- Wählen Sie im Menü **Algorithmus** den Verschlüsselungsalgorithmus für den Schutz des PGP Virtual Disk-Laufwerks aus: **AES-256 (256 Bit)**, **CAST5 (128 Bit)** oder **EME2-AES (256 Bit)**. Weitere Informationen zu diesen Verschlüsselungsalgorithmen finden Sie unter PGP Virtual Disk-Verschlüsselungsalgorithmen.
- Wählen Sie im Menü **Format** das Laufwerksformat für das PGP Virtual Disk-Laufwerk aus:

  MS-DOS: Verwenden Sie dieses Format, wenn Sie das PGP Virtual Disk-Laufwerk mit PGP Desktop 10.1 für Windows gemeinsam mit anderen Personen verwenden möchten.

  Mac OS Extended: Dies ist das Standardformat (und entspricht dem modernen Mac OS-Dateisystemformat), das große PGP Virtual Disk-Laufwerke unterstützt. Die Mindestgröße beträgt 4 MB. Das Format „Mac OS Extended“ wird auch als HFS+ bezeichnet.

Mac OS Extended (im Journal erfasst): Verwenden Sie dieses Format, wenn die Journalerstellung auf dem System aktiviert ist. (Bei der Journalerstellung werden alle Daten, die auf die Festplatte geschrieben werden, in Form einer zusätzlichen Kopie in einem privaten Bereich des Dateisystems abgelegt, um eine eventuell erforderliche Wiederherstellung zu erleichtern.)

Mac OS Extended (Groß-/Kleinschreibung-Unterscheidung, im Journal erfasst): Verwenden Sie dieses Format, wenn die Journalerstellung mit Beachtung der Groß-/Kleinschreibung auf dem System aktiviert ist.

Mac OS Standard: Dieses Format dient der Rückwärtskompatibilität mit älteren Mac OS-Betriebssystemen. Die Mindestgröße beträgt 512 KB.

UNIX-Dateisystem: Verwenden Sie dieses Format, wenn Sie das PGP Virtual Disk-Laufwerk mit UNIX-Benutzern gemeinsam verwenden möchten. Die Mindestgröße beträgt 128 KB.

Sie können unter Mac OS X das Format eines Laufwerks anzeigen, indem Sie dieses auswählen und im Menü „Ablage“ auf „Informationen“ klicken.

6 Klicken Sie auf **Fortfahren**.

7 Der nächste Schritt richtet sich danach, welcher Authentifizierungstyp (öffentlicher Schlüssel oder Passphrase) ausgewählt wurde.

- Wenn Sie „Öffentlicher Schlüssel“ ausgewählt haben, wird der Bildschirm „Öffentlichen Schlüssel zum Sichern des PGP-Laufwerks auswählen“ mit den öffentlichen Schlüsseln angezeigt, die Sie für die Authentifizierung am erstellten PGP Virtual Disk-Laufwerk verwenden können.

  Wählen Sie einen Schlüssel aus der Liste aus und klicken Sie auf **Fortfahren**. Sie werden aufgefordert, die Passphrase für den ausgewählten Schlüssel einzugeben (sofern die Passphrase nicht zwischengespeichert ist, sodass dieser Schritt übersprungen wird).

  Geben Sie die Passphrase ein und klicken Sie auf **OK**. Das Dialogfeld „Speichern unter“ wird angezeigt. Fahren Sie mit dem nächsten Schritt fort.

- Wenn Sie die Passphrasenoption ausgewählt haben, wird der Bildschirm „Hauptpassphrase für das PGP-Laufwerk festlegen“ angezeigt.

  Geben Sie in das Feld **Name** den Namen für den primären PGP Virtual Disk-Benutzer (oder den Administrator) ein.

  Geben Sie in das Feld **Passphrase eingeben** die gewünschte Passphrase ein. Die **Passphrasen-Qualitätsanzeige** zeigt die Stärke der eingegebenen Passphrase an. Aktivieren Sie das Kontrollkästchen **Tastatureingabe anzeigen**, wenn die eingegebenen Zeichen angezeigt werden sollen und Sie sicher sind, dass Sie nicht beobachtet werden.

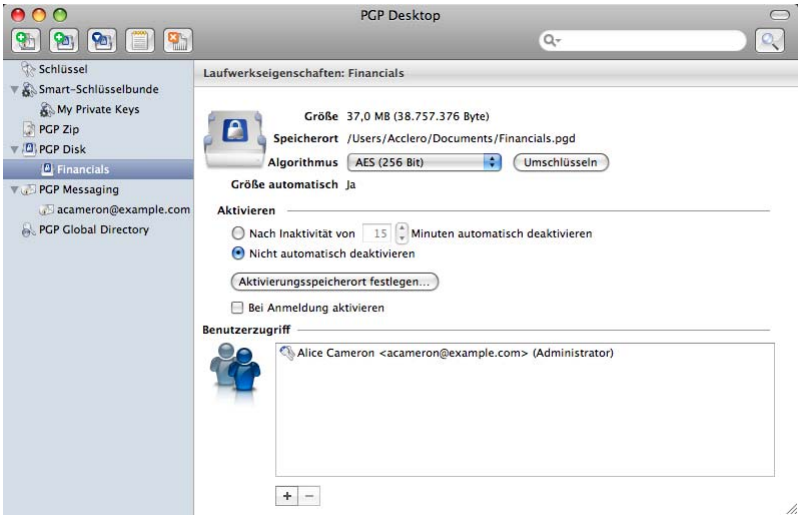
Geben Sie die Passphrase in das Feld **Passphrase anzeigen** erneut ein. Klicken Sie auf **Fortfahren**. Das Dialogfeld „Speichern unter“ wird angezeigt. Fahren Sie mit dem nächsten Schritt fort.

8 Wählen Sie einen Dateinamen und einen Speicherort für das PGP Virtual Disk-Laufwerk aus und klicken Sie auf **Speichern**.

9 Überprüfen Sie die Informationen im Bildschirm „Übersicht über die PGP-Laufwerkserstellung“. In diesem Bildschirm werden die Größe des PGP Virtual Disk-Laufwerks, der Name und der Speicherort des Laufwerks, das Format usw. angezeigt. Klicken Sie anschließend auf **Erstellen**.

10 Im Bildschirm für die Erstellung des PGP Virtual Disk-Laufwerks wird der Fortschritt des Vorgangs angezeigt. Sobald die Erstellung abgeschlossen ist, wird der Bildschirm „Herzlichen Glückwunsch“ angezeigt. Klicken Sie auf **Beenden**.

11 Das neue PGP Virtual Disk-Laufwerk wird automatisch aktiviert und in einem Finder-Fenster werden Informationen zu diesem Laufwerk angezeigt. Der Name des Laufwerks wird ebenfalls unter **PGP Disk** angezeigt.



Eigenschaften von PGP Virtual Disk-Laufwerken anzeigen

Nachdem Sie ein PGP Virtual Disk-Laufwerk erstellt haben, können Sie im Bildschirm „Laufwerkseigenschaften“ auf Informationen zum Laufwerk sowie zu den Einstellungen zugreifen, die geändert werden können.

So zeigen Sie die Eigenschaften eines PGP Disk-Laufwerks an

- Klicken Sie im Bedienfeld **PGP Disk** auf den Namen des Laufwerks. Der Bildschirm „Laufwerkseigenschaften“ wird angezeigt.

Aktivierte PGP Virtual Disk-Laufwerke verwenden

Sie können Dateien und Ordner auf einem PGP Virtual Disk-Laufwerk wie auf jedem anderen Laufwerk des Systems erstellen, kopieren, verschieben und löschen.

Andere Personen mit Zugriff auf das Laufwerk (entweder auf demselben Computer oder über ein Netzwerk) können ebenfalls auf die darauf gespeicherten Daten zugreifen. Die Daten werden erst geschützt, wenn Sie das Laufwerk deaktivieren.

Achtung: Obwohl die PGP Virtual Disk-Laufwerksdatei verschlüsselt und vor unbefugtem Zugriff geschützt ist, kann sie dennoch von der Festplatte gelöscht werden. Alle Personen mit Zugriff auf Ihr System könnten die verschlüsselte Datei mit dem PGP Virtual Disk-Laufwerk löschen. Daher sollten Sie eine Sicherungskopie der verschlüsselten Datei aufbewahren und den Computer sperren, wenn Sie nicht in der Nähe sind.

PGP Virtual Disk-Laufwerke aktivieren

Wenn Sie ein neues PGP Virtual Disk-Laufwerk erstellen, wird es automatisch aktiviert, sodass Sie es sofort zum Speichern von Dateien einsetzen können.

Damit Sie den Inhalt eines Laufwerks sichern können, müssen Sie es deaktivieren. Nach dem Deaktivieren des Laufwerks sind die Daten sicher in einer verschlüsselten Datei gespeichert und der Zugriff ist erst möglich, wenn das Laufwerk wieder aktiviert wird.

Es gibt verschiedene Möglichkeiten, ein PGP Virtual Disk-Laufwerk zu aktivieren:

- Wählen Sie in PGP Desktop das PGP Virtual Disk-Laufwerk aus, das Sie aktivieren möchten, und wählen Sie **Laufwerk > Aktivieren** aus.
- Wählen Sie in PGP Desktop das PGP Virtual Disk-Laufwerk aus, das Sie aktivieren möchten, und klicken Sie unter Windows in der oberen rechten Ecke auf **Aktivieren** oder unter Mac OS X in der Symbolleiste auf das Symbol **Aktivieren**.
- Ändern Sie die Eigenschaften des PGP Virtual Disk-Laufwerks, sodass es beim Start des Computers aktiviert wird.

Nur unter Windows:

- Aktivieren Sie während der Erstellung des PGP Virtual Disk-Laufwerks das Kontrollkästchen **Beim Start aktivieren**. Das Laufwerk wird dann beim Start von Windows automatisch aktiviert. Wenn Sie diese Option nicht beim Erstellen des PGP Virtual Disk-Laufwerks aktivieren, können Sie dies später nachholen.

- Klicken Sie in Windows Explorer mit der rechten Maustaste auf die PGP Virtual Disk-Datei und wählen Sie im Kontextmenü die Option **PGP > PGP Virtual Disk-Laufwerk aktivieren** aus.

Aktivierte PGP Virtual Disk-Laufwerke werden in Windows Explorer und im Finder von Mac OS X als leere Laufwerke angezeigt.

PGP Virtual Disk-Laufwerke deaktivieren

Sie können ein PGP Virtual Disk-Laufwerk sperren, indem Sie es deaktivieren. Nach dem Deaktivieren eines PGP Virtual Disk-Laufwerks ist dessen Inhalt in der verschlüsselten Laufwerksdatei gesperrt. Der Inhalt ist erst dann wieder zugänglich, wenn das Laufwerk wieder aktiviert wird.

Achtung: Wenn Sie ein PGP Virtual Disk-Laufwerk deaktivieren und darauf gespeicherte Dateien geöffnet sind, können Daten verloren gehen. Geben Sie Optionen für die Deaktivierung von Laufwerken an, indem Sie **PGP > Einstellungen** auswählen und auf das Symbol **Laufwerk** klicken. Eine Option lautet **Deaktivierung von PGP-Laufwerken zulassen, wenn Dateien geöffnet sind**. Wenn diese Option ausgewählt ist, ist auch die Option für **Keine Bestätigung zum Deaktivieren anfordern** verfügbar. **Verwenden Sie diese Optionen nur, wenn Sie damit vertraut sind.** Diese Optionen sind zwar für fortgeschrittene Benutzer hilfreich, die Ihre Daten regelmäßig sichern, sind jedoch für die meisten Benutzer nicht zu empfehlen.

Es gibt verschiedene Möglichkeiten, ein PGP Virtual Disk-Laufwerk zu deaktivieren:

- Wählen Sie in PGP Desktop im Bedienfeld „PGP Disk“ das PGP Virtual Disk-Laufwerk aus, das Sie deaktivieren möchten, und klicken Sie auf **Laufwerk > Deaktivieren**. Sie können auch in der Symbolleiste auf das Symbol **Laufwerk deaktivieren** **klicken.**
- Ziehen Sie das Symbol des aktivierten PGP Virtual Disk-Laufwerks in den **Papierkorb**.

Aktivierungsspeicherort festlegen

Sie können festlegen, wo das PGP Virtual Disk-Laufwerk aktiviert (gespeichert) wird.

So legen Sie den Aktivierungsspeicherort fest

1. Klicken Sie auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual-Laufwerk aus, dessen Aktivierungsspeicherort Sie festlegen möchten.
2. Klicken Sie auf **Aktivierungsspeicherort festlegen**. Das Dialogfeld „Aktivierungspunkt des PGP-Laufwerks festlegen“ wird angezeigt.
3. Wählen Sie eine der folgenden Optionen aus:

- **Desktop (Standard)**: Wählen Sie diese Option aus, wenn das PGP Disk-Laufwerk auf dem Desktop aktiviert werden soll. Hier wird das PGP Virtual Disk-Laufwerk auch aktiviert, wenn Sie keinen anderen Speicherort angeben.
- **Am folgenden Speicherort**: Wählen Sie diese Option aus, um das PGP Virtual Disk-Laufwerk am angegebenen Speicherort zu aktivieren. Klicken Sie auf **Durchsuchen** **und wechseln Sie zum dem Speicherort, an dem das PGP Virtual Disk-Laufwerk aktiviert werden soll. Klicken Sie auf** **Öffnen**, um die Auswahl zu bestätigen.

4 Klicken Sie auf **OK**. Der Aktivierungsspeicherort für das PGP Virtual Disk-Laufwerk wurde festgelegt.

PGP Virtual Disk-Laufwerke komprimieren

Sie können zusätzlichen Speicherplatz auf dem PGP Virtual Disk-Laufwerk freigeben, indem Sie das Laufwerk komprimieren. Wenn das PGP Virtual Disk-Laufwerk aktiviert ist, müssen Sie das Laufwerk zunächst deaktivieren, bevor es komprimiert werden kann.

So komprimieren Sie ein PGP Virtual Disk-Laufwerk

- Führen Sie einen der folgenden Schritte aus:
  - Wechseln Sie im Finder unter Mac OS X zum Speicherort der PGD-Datei. Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **PGP > Komprimieren** aus.

    Wenn Sie sich bezüglich des Speicherorts des PGP Virtual Disk-Laufwerks nicht sicher sind, klicken Sie in PGP Desktop mit der rechten Maustaste auf den Namen des Laufwerks und wählen Sie die Option **Im Finder anzeigen** aus.
  - Klicken Sie in PGP Desktop im linken Bereich des Hauptbildschirms von PGP Desktop auf „PGP Disk“, wählen Sie das PGP Virtual Disk-Laufwerk aus, das Sie komprimieren möchten, und wählen Sie anschließend die Option **Laufwerk > Laufwerk komprimieren** aus. Sie können auch die Ctrl-Taste gedrückt halten und im Bedienfeld „PGP Disk“ auf das PGP Virtual Disk-Laufwerk klicken (bzw. bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste klicken) und im Kontextmenü die Option **Komprimieren** auswählen.

PGP Virtual Disk-Laufwerke umschlüsseln

Sie können die auf einem PGP Virtual Disk-Laufwerk gespeicherten Daten umschlüsseln. Dies kann aus einem von zwei (oder beiden) Gründen erfolgen:

- Sie möchten den Verschlüsselungsalgorithmus ändern, mit dem das Laufwerk derzeit geschützt ist.
- Sie vermuten, dass ein Sicherheitsverstoß aufgetreten ist.

Bei der Umschlüsselung wird das PGP Virtual Disk-Laufwerk erneut verschlüsselt, jedoch wird ein anderer zugrunde liegender Verschlüsselungsschlüssel verwendet.

Achtung: Erfahrene Benutzer können in der Lage sein, den Speicher eines Computers nach dem zugrunde liegenden Verschlüsselungsschlüssel eines PGP Virtual Disk-Laufwerks zu durchsuchen. Diese Benutzer könnten den Schlüssel für den Zugriff auf das Laufwerk verwenden, nachdem sie aus der Benutzerliste gelöscht wurden. Bei der Umschlüsselung des Laufwerks wird dieser zugrunde liegende Schlüssel geändert und ein derartiger unberechtigter Eingriff verhindert.

So schlüsseln Sie ein PGP Virtual Disk-Laufwerk um

1. Klicken Sie im linken Bereich des Hauptbildschirms von PGP Desktop auf „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk aus, das Sie umschlüsseln möchten.
2. Deaktivieren Sie das PGP Virtual Disk-Laufwerk, falls es aktiviert ist.
3. Klicken Sie auf **Umschlüsseln**. Ein Bestätigungsdialogfeld wird angezeigt.
4. Überprüfen Sie die aufgeführten Informationen und klicken Sie auf **Umschlüsseln**. Das Dialogfeld „PGP-Passphrase eingeben“ wird angezeigt.
5. Geben Sie die Passphrase des PGP Virtual Disk-Administrators ein und klicken Sie auf **OK**. Das PGP Virtual Disk-Laufwerk wird umgeschlüsselt. Während des Vorgangs wird eine Fortschrittsanzeige eingeblendet.
6. Wenn der aktuelle Status „Fertig“ lautet, klicken Sie auf **Weiter**.
7. Klicken Sie auf **Beenden**, um die Umschlüsselung abzuschließen.

Mit anderen Benutzern arbeiten

In diesem Abschnitt wird beschrieben, wie Konten anderer Benutzer für PGP Virtual Disk-Laufwerke hinzugefügt, gelöscht und deaktiviert werden. Darüber hinaus finden Sie hier Informationen zum Ändern der Rechte von Benutzern, einschließlich der Gewährung von Administratorrechten für einen Benutzer.

Konten anderer Benutzer zu einem PGP Virtual Disk-Laufwerk hinzufügen

Der Administrator eines PGP Virtual Disk-Laufwerks kann das Laufwerk anderen Benutzern zugänglich machen. Diese Benutzer können dann mit ihrer eigenen Passphrase oder ihrem eigenen privaten Schlüssel auf das Laufwerk zugreifen.

So fügen Sie einem PGP Virtual Disk-Laufwerk Konten anderer Benutzer hinzu

1. Klicken Sie im linken Fensterbereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie den Namen des PGP Virtual Disk-Laufwerks aus, dem Sie einen anderen Benutzer hinzufügen möchten.
2. Klicken Sie im Bildschirm „Laufwerkseigenschaften“ auf das Plussymbol unter der Liste „Benutzerzugriff“. Wählen Sie abhängig von der Art des Kontos anderer Benutzer, das Sie hinzufügen möchten, die Option **Benutzer öffentlicher Schlüssel hinzufügen** **oder** **Passphrasenbenutzer hinzufügen** **aus.**
   - Wenn Sie **Benutzer öffentlicher Schlüssel hinzufügen** ausgewählt haben, wählen Sie den öffentlichen Schlüssel des anderen Benutzers aus, den Sie hinzufügen möchten. Ziehen Sie hierzu den Schlüssel aus der Spalte **Schlüsselquelle** in die Spalte **Hinzuzufügende Schlüssel**. Sie können bei Bedarf mehrere andere Benutzer hinzufügen.
   - Wenn Sie **Passphrasenbenutzer hinzufügen** ausgewählt haben, wählen Sie den öffentlichen Schlüssel des anderen Benutzers aus, den Sie hinzufügen möchten. Ziehen Sie hierzu den Schlüssel aus der Spalte **Schlüsselquelle** in die Spalte **Hinzuzufügende Schlüssel**. Das Dialogfeld „Benutzer zu PGP-Laufwerk hinzufügen“ wird angezeigt.

     Geben Sie in das Feld **Name** den Namen des anderen Benutzers ein.

     Geben Sie in das Feld **Passphrase für diesen Benutzer eingeben** eine Passphrase für den Benutzer ein.

     Wiederholen Sie die Eingabe der Passphrase im Feld **Passphrase des Benutzers bestätigen**. Die **Passphrasen-Qualitätsanzeige** zeigt die Stärke der eingegebenen Passphrase an. Wenn die Zeichen der Passphrase während der Eingabe angezeigt werden sollen, aktivieren Sie das Kontrollkästchen **Tastatureingabe anzeigen**.
3. Klicken Sie auf **OK**. Der Bildschirm „Laufwerkseigenschaften“ wird erneut angezeigt, wobei der andere Benutzer des öffentlichen Schlüssels bzw. der andere Passphrasenbenutzer in der Liste aufgeführt wird.

Konten anderer Benutzer von einem PGP Virtual Disk-Laufwerk löschen

Gelegentlich kann es erforderlich sein, einem Benutzer den Zugriff auf ein PGP Virtual Disk-Laufwerk zu entziehen.

So entfernen Sie das Konto eines anderen Benutzers von einem PGP Virtual Disk-Laufwerk:

1. Klicken Sie im linken Bereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk für das Benutzerkonto aus, das Sie löschen möchten.
2. Wählen Sie in der Liste „Benutzerzugriff“ den Namen des anderen Benutzers aus, dessen Konto Sie entfernen möchten. Der Administrator kann nicht entfernt werden.
3. Klicken Sie auf das Minussymbol unter der Liste **Benutzerzugriff**. Ein Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf **Entfernen**. Der andere Benutzer wird gelöscht.

Konten anderer Benutzer deaktivieren und aktivieren

Sie können den Zugriff eines Benutzers auf ein PGP Virtual Disk-Laufwerk vorübergehend verhindern, ohne dessen Konto komplett zu entfernen, indem Sie stattdessen das Konto deaktivieren.

So deaktivieren oder aktivieren Sie Konten anderer Benutzer auf einem PGP Virtual Disk-Laufwerk:

1. Klicken Sie im linken Bereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk für das Benutzerkonto aus, das Sie ändern möchten.
2. Wählen Sie in der Liste **Benutzerzugriff** den anderen Benutzer aus, den Sie deaktivieren oder aktivieren möchten. Der Administrator kann nicht deaktiviert werden.
3. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie einen Benutzer deaktivieren möchten, wählen Sie **Laufwerk > Benutzer deaktivieren** aus. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Deaktiviert**. Der andere Benutzer wird deaktiviert. Der Benutzer wird in der Liste **Benutzerzugriff** grau dargestellt.
   - Wenn Sie einen Benutzer aktivieren möchten, den Sie zuvor deaktiviert haben, klicken Sie auf **Laufwerk > Benutzer aktivieren**. Der andere Benutzer wird aktiviert.

Lese-/Schreib- und Schreibschutzstatus ändern

Benutzer von PGP Virtual Disk-Laufwerken können entweder über vollständigen Lese-/Schreibzugriff oder nur über Lesezugriff verfügen. Diese Berechtigung kann jederzeit für Benutzer geändert werden.

▸ **So ändern Sie die Berechtigungen für einen Benutzer eines PGP Virtual Disk-Laufwerks**

1. Klicken Sie im linken Bereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk für das Benutzerkonto aus, das Sie ändern möchten.
2. Wählen Sie in der Liste „Benutzerzugriff“ den Namen des anderen Benutzers aus, dessen Lese-/Schreibstatus Sie ändern möchten.
3. Führen Sie einen der folgenden Schritte aus:
   - Wenn der Benutzer nur über Leseberechtigungen verfügen soll, klicken Sie bei gedrückter Ctrl-Taste (oder mit der rechten Maustaste) auf den Namen des jeweiligen Benutzers und wählen Sie die Option **Schreibgeschützten Zugriff festlegen** aus.
   - Wenn der Benutzer über Lese- und Schreibberechtigungen verfügen soll, klicken Sie bei gedrückter Ctrl-Taste (oder mit der rechten Maustaste) auf den Namen des jeweiligen Benutzers und wählen Sie die Option **Schreibzugriff erlauben** aus.

   Tipp: Diese Optionen stehen auch im Menü „Laufwerk“ zur Verfügung, wenn der Benutzer ausgewählt wurde.
4. Die Rechte des ausgewählten Benutzers sind nun geändert.

Anderen Benutzern Administratorstatus gewähren

Sie können den Status eines Benutzerkontos ändern und aus einem anderen Benutzer einen Administrator machen.

▸ **So gewähren Sie Administratorstatus:**

1. Klicken Sie im linken Bereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk für das Benutzerkonto aus, das Sie ändern möchten.

2 Wählen Sie in der Liste „Benutzerzugriff“ den Benutzer aus, den Sie zum Administrator des PGP Virtual Disk-Laufwerks machen möchten. Wählen Sie entweder einen Passphrasenbenutzer oder sich selbst (wenn Sie nicht der aktuelle Administrator sind). Beachten Sie, dass Sie keinen Benutzer eines öffentlichen Schlüssels zum Administrator des PGP Virtual Disk-Laufwerks machen können.

3 Klicken Sie mit gedrückter Ctrl-Taste (bzw. bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste) und wählen Sie aus dem Kontextmenü die Option **Als Laufwerksadministrator festlegen** aus. Das Dialogfeld „PGP-Passphrase eingeben“ wird angezeigt.

Tipp: Sie können auch auf **Laufwerk > Als Laufwerksadministrator festlegen** **klicken.**

4 Geben Sie die Passphrase des PGP Virtual Disk-Administrators ein und klicken Sie auf **OK**. Das ausgewählte Benutzerkonto wird auf Administrator geändert.

Hinweis: Sie können immer nur einem Benutzerkonto den Administratorstatus zuweisen. Durch Zuweisen des Administratorstatus zu einem Konto wird dieser Status automatisch von einem anderen Konto entfernt.

Benutzer-Passphrasen ändern

So ändern Sie die Benutzer-Passphrase für ein PGP Virtual Disk-Laufwerk

1 Klicken Sie im linken Bereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk aus, für das Sie ein Benutzer sind.

2 Wählen Sie aus der Liste „Benutzerzugriff“ den Namen des Passphrasenbenutzers aus und klicken Sie im Menü **Laufwerk** auf **Benutzerpassphrase ändern**. Das Dialogfeld „PGP-Passphrase eingeben“ wird angezeigt.

Tipp: Sie können auch bei gedrückter Ctrl-Taste (bzw. bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste) auf den Namen des Benutzers klicken und im Kontextmenü die Option **Benutzerpassphrase ändern** auswählen.

3 Geben Sie die Passphrase des PGP Virtual Disk-Administrators ein und klicken Sie auf **OK**.

4 Geben Sie eine neue Passphrase ein. Geben Sie sie zur Bestätigung noch einmal ein, und klicken Sie auf **OK**. Die Passphrase wird geändert.

PGP Virtual Disk-Laufwerke löschen

Möglicherweise stellen Sie irgendwann fest, dass Sie ein bestimmtes PGP Virtual Disk-Laufwerk nicht mehr benötigen und entscheiden sich, das gesamte Laufwerk zu löschen.

Achtung: Beim Löschen eines PGP Virtual Disk-Laufwerks werden auch alle darauf befindlichen Daten gelöscht. *Es gibt keine Möglichkeit, die Daten wiederherzustellen, nachdem ein PGP Virtual Disk-Laufwerk gelöscht wurde.* Stellen Sie sicher, dass Sie alle Daten, die Sie speichern möchten, an einen anderen Speicherort kopiert haben, *bevor Sie ein PGP Virtual Disk-Laufwerk löschen.*

Stellen Sie sicher, dass das PGP Virtual Disk-Laufwerk *nicht* aktiviert ist. Ein aktiviertes PGP Virtual Disk-Laufwerk kann nicht gelöscht werden.

So löschen Sie ein PGP Virtual Disk-Laufwerk

1. Klicken Sie im linken Fensterbereich des Hauptbildschirms von PGP Desktop auf das Bedienfeld „PGP Disk“ und wählen Sie das PGP Virtual Disk-Laufwerk aus, das Sie löschen möchten.
2. Klicken Sie im Kontextmenü auf **Im Finder anzeigen**. Es wird ein Finder-Fenster mit der ausgewählten PGP Virtual Disk-Laufwerksdatei angezeigt. Wenn Sie Mac OS X für die Anzeige von Dateiendungen konfiguriert haben, wird die PGP Virtual Disk-Laufwerksdatei mit der Endung „.pgd“ angezeigt.
3. Ziehen Sie die Datei in den Papierkorb und klicken Sie im Finder im Menü „Ablage“ auf **Papierkorb entleeren**.
4. Klicken Sie in PGP Desktop bei gedrückter Ctrl-Taste (oder bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste) auf das PGP-Laufwerk, das Sie löschen möchten, und wählen Sie aus dem Kontextmenü die Option **Element entfernen** aus. Das PGP-Laufwerk wird vom System sowie aus PGP Desktop entfernt.

PGP Virtual Disk-Laufwerke warten

In diesem Abschnitt wird die ordnungsgemäße Handhabung von PGP Virtual Disk-Laufwerken beschrieben, die Sie mit Ihrem Computer verwenden.

PGP Virtual Disk-Laufwerke auf einem Remoteserver aktivieren

PGP Virtual Disk-Laufwerke können auf jeder Art von Server (Windows oder UNIX) platziert werden. Die Laufwerke können dann von jedem Benutzer mit einem Windows-Computer und PGP Desktop aktiviert werden.

Hinweis: Die erste Person, die das PGP Virtual Disk-Laufwerk lokal aktiviert, erhält Lese-/Schreibzugriff auf das Laufwerk. Danach können keine weiteren Personen auf das Laufwerk zugreifen. Wenn Sie den Zugriff durch andere Personen zulassen möchten, müssen Sie das Laufwerk im schreibgeschützten Modus aktivieren (gilt nur für FAT- und FAT32-Dateisysteme). Alle Benutzer des Laufwerks verfügen dann ausschließlich über Lesezugriff.

Wenn das PGP Virtual Disk-Laufwerk auf einem Windows-Server gespeichert ist, können Sie das Laufwerk auch remote auf dem Server aktivieren und anderen Personen die Freigabe des aktivierten Laufwerks gestatten. Dieses Verfahren bietet jedoch keinen Schutz für die Dateien auf dem Laufwerk.

Sicherungskopien von PGP Virtual Disk-Laufwerken erstellen

Sie können Daten am besten vor Hardwarefehlern oder sonstigem Verlust schützen, indem Sie Sicherungskopien des Inhalts der PGP Virtual Disk-Laufwerke erstellen.

Es empfiehlt sich nicht, den Inhalt eines aktivierten (und daher entschlüsselten) PGP Virtual Disk-Laufwerks wie jedes andere Laufwerk zu sichern. Der Inhalt ist nicht verschlüsselt und daher für jeden zugänglich, der die Sicherungskopie wiederherstellen kann. Erstellen Sie stattdessen eine Sicherungskopie des verschlüsselten Laufwerks.

So erstellen Sie eine Sicherungskopie eines verschlüsselten PGP Virtual Disk-Laufwerks

1. Deaktivieren Sie das PGP Virtual Disk-Laufwerk.
2. Wechseln Sie im Finder zur PGP Virtual Disk-Laufwerksdatei. Wenn Sie Mac OS X für die Anzeige der Dateiendungen konfiguriert haben, weist der Name der Laufwerksdatei die Endung `.pgd` auf.

   Tipp: Sie können die PGP Virtual Disk-Datei problemlos finden, indem Sie im PGP Desktop-Fenster im Bedienfeld „PGP Disk“ bei gedrückter Ctrl-Taste (oder bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste) auf das Laufwerk klicken. Klicken Sie im Kontextmenü auf **Im Finder anzeigen**.
3. Kopieren Sie die deaktivierte verschlüsselte PGP Virtual Disk-Laufwerksdatei wie jede andere Datei auf eine CD, eine DVD, ein Band, ein Steckmodul oder eine Diskette.

Selbst wenn eine unbefugte Person Zugriff auf die Sicherungskopie erhält, kann sie den Inhalt nicht entschlüsseln.

Wenn Sie Sicherungskopien von verschlüsselten PGP Virtual Disk-Dateien erstellen, sollten Sie Folgendes beachten:

- Das Erstellen von Sicherungskopien der verschlüsselten Dateien auf einem Netzlaufwerk bietet anderen Personen ausreichend Gelegenheit, eine schwache Passphrase zu erraten. Es ist bedeutend sicherer, Sicherungskopien nur auf Geräten zu erstellen, die sich physisch in Ihrem Besitz befinden.
- Eine lange und komplizierte Passphrase verbessert die Sicherheit Ihrer Daten zusätzlich.
- Wenn Sie in einem Netzwerk arbeiten, achten Sie darauf, dass die Dateien auf Ihrem *aktivierten* PGP Virtual Disk-Laufwerk nicht durch ein Netzwerksicherungssystem gesichert werden. (Wenden Sie sich ggf. an den Systemadministrator.) Nach der Aktivierung eines PGP Virtual Disk-Laufwerks sind dessen Dateien entschlüsselt und können in diesem Zustand auf ein Netzwerksicherungssystem kopiert werden.

PGP Virtual Disk-Laufwerke austauschen

Sie können PGP Virtual Disk-Laufwerke mit anderen Benutzern austauschen, die auf ihren Computern PGP Desktop installiert haben. Dazu senden Sie diesen Personen eine Kopie der Datendatei des PGP Virtual Disk-Laufwerks, die die Laufwerksdaten enthält. PGP Virtual Disk-Laufwerke können u. a. folgendermaßen ausgetauscht werden:

- Als E-Mail-Anlagen
- Auf einem Wechseldatenträger oder auf CDs
- Über ein Netzwerk

Nachdem der andere Benutzer die PGP Virtual Disk-Laufwerksdatei erhalten hat, kann dieser sie auf einem System mit PGP Desktop aktivieren und unter Verwendung der richtigen Passphrase darauf zugreifen. Wenn das Laufwerk an ihren öffentlichen Schlüssel verschlüsselt wurde, würden sie ihren privaten Schlüssel für den Zugriff verwenden.

Hinweis: Der öffentliche Schlüssel ist aus folgenden Gründen die sicherste Schutzmethode beim Hinzufügen anderer Benutzer zu einem PGP Virtual Disk-Laufwerk: (1) Sie müssen keine Passphrase mit dem anderen Benutzer austauschen, die, abhängig von der Austauschmethode, abgefangen oder abgehört werden könnte. (2) Der andere Benutzer muss sich keine weitere Passphrase merken, die er vergessen könnte. (3) Die Verwaltung einer Liste von Benutzern wird vereinfacht, wenn jeder Benutzer einen eigenen privaten Schlüssel zum Entsperren des Laufwerks verwendet.

PGP Virtual Disk-Verschlüsselungsalgorithmen

Bei der Verschlüsselung wird eine mathematische Formel zum Chiffrieren von Daten eingesetzt, damit sie von anderen Personen nicht verwendet werden können. Wenn Sie den richtigen mathematischen Schlüssel anwenden, werden die Daten wieder dechiffriert. Die Verschlüsselungsformel für PGP Virtual Disk-Laufwerke verwendet für einen Teil des Verschlüsselungsvorgangs Zufallsdaten.

Die PGP Desktop-Anwendung bietet starke Algorithmusoptionen zum Schutz von PGP Virtual Disk-Laufwerken: AES-256, CAST und Twofish.

- Der erweiterte Verschlüsselungsstandard AES (Advanced Encryption Standard) ist der von NIST genehmigte Verschlüsselungsstandard. Der zugrunde liegende Algorithmus ist Rijndael, ein von Joan Daemen und Vincent Rijmen entwickelter Block-Algorithmus. AES ersetzt den vorherigen Datenverschlüsselungsstandard DES (Data Encryption Standard). PGP Virtual Disk-Laufwerke können mit der stärksten Variation von AES, AES-256 (d. h. AES mit einer Schlüsselgröße von 256 Bit) geschützt werden.
- CAST gilt als ausgezeichneter Block-Algorithmus, da er schnell auszuführen, jedoch nur schwer zu entziffern ist. Der Name ist von den Initialen der Entwickler Carlisle Adams und Stafford Tavares von Northern Telecom (Nortel) abgeleitet. Nortel hat ein Patent für CAST angemeldet, verpflichtet sich jedoch, CAST ohne Lizenzgebühren für jedermann verfügbar zu machen. Bei CAST scheint es sich um einen Algorithmus zu handeln, der von Spezialisten mit hervorragendem Ruf innerhalb der Branche außergewöhnlich gut entwickelt wurde.

  Das Design basiert auf einem sehr formellen Ansatz und enthält eine Reihe formal nachweisbarer Behauptungen, die Grund zu der Annahme geben, dass alle Schlüssel geprüft werden müssten, bevor der 128-Bit-Schlüssel entziffert würde. CAST hat keine schwachen Schlüssel. Es gibt überzeugende Argumente dafür, dass CAST gegen lineare und differenziale Kryptanalyse immun ist, die zwei leistungsstärksten Formen von Kryptanalyse in der veröffentlichten Literatur. Beide haben sich beim Knacken von DES als effektiv erwiesen.

  EME2-AES (256 Bit) ist ein stärkerer Algorithmus, der jeden Vorgang doppelt verschlüsselt. EME2 (Encrypt-Mix-Encrypt v2) ist ein Wide-Block-Algorithmus, der derzeit von der Arbeitsgruppe für IEEE-Standards geprüft wird.

Spezielle Sicherheitsfunktionen von PGP Virtual Disk

Im Gegensatz zu manchen anderen Programmen legt PGP Desktop besonderen Wert auf die Vermeidung von Sicherheitsproblemen mit PGP Virtual Disk-Laufwerken.

Diese Sicherheitsmaßnahmen gelten auch für vollständig verschlüsselte Laufwerke.

Löschung der Passphrase

Wenn Sie eine Passphrase eingeben, wird diese von PGP Desktop nur für kurze Zeit verwendet und danach aus dem Speicher gelöscht. PGP Desktop erstellt außerdem keine Kopien der Passphrase. Daher befindet sich die Passphrase in der Regel nur für den Bruchteil einer Sekunde im Speicher. Diese Funktion ist von größter Bedeutung, da sonst andere Personen im Hauptspeicher nach der Passphrase suchen könnten, während Sie nicht an Ihrem Arbeitsplatz sind. Diese Personen würden dann ohne Ihr Wissen vollständigen Zugriff auf alle mit dieser Passphrase geschützten Daten erhalten.

Schutz des virtuellen Speichers

Ihre Passphrase oder andere Schlüssel könnten mit den Daten des virtuellen Speichersystems auf die Festplatte ausgelagert werden. PGP Desktop lässt jedoch nicht zu, dass die Passphrasen und Schlüssel auf die Festplatte geschrieben werden. Mit dieser Funktion wird verhindert, dass unberechtigte Personen die virtuelle Speicherdatei nach Passphrasen durchsuchen.

Schutz durch MSIM (Memory Static Ion Migration)

Wenn Sie ein PGP Virtual Disk-Laufwerk aktivieren, wird die Passphrase in einen Schlüssel umgewandelt. Dieser Schlüssel dient zum Verschlüsseln und Entschlüsseln der Daten auf dem PGP Virtual Disk-Laufwerk. Obwohl die Passphrase sofort aus dem Speicher gelöscht wird, bleibt der Schlüssel (aus dem die Passphrase nicht abgeleitet werden kann) jedoch im Speicher erhalten, während das Laufwerk aktiviert ist.

Dieser Schlüssel wird zwar nicht im virtuellen Speicher gespeichert, wenn jedoch ein bestimmter Speicherbereich genau dieselben Daten für extrem lange Zeiträume speichert, ohne dass der Computer ausgeschaltet oder zurückgesetzt wird, bleibt eine statische Ladung im Speicher zurück, die von Angreifern gelesen werden könnte. Wenn das PGP Virtual Disk-Laufwerk für längere Zeit aktiviert bleibt, können mit der Zeit erkennbare Spuren des Schlüssels im Speicher zurückbleiben. Mit bestimmten Geräten könnte der Schlüssel wiederhergestellt werden. Diese Geräte sind zwar nicht im Elektronikfachgeschäft um die Ecke zu finden, stehen wahrscheinlich jedoch größeren Regierungsbehörden zur Verfügung.

PGP Desktop schützt vor derartigen Angriffen, indem zwei Kopien (eine normale Kopie und eine Kopie mit umgekehrten Bit) im RAM-Speicher gehalten und alle paar Sekunden umgekehrt werden.

Weitere Sicherheitsaspekte

Im Allgemeinen hängt die Fähigkeit zum Schützen von Daten von den Vorkehrungen ab, die Sie treffen. Kein Verschlüsselungsprogramm kann Sie vor unzureichenden Sicherheitsmaßnahmen schützen. Wenn Sie sich z. B. vom Schreibtisch entfernen und dabei den Computer eingeschaltet und vertrauliche Dateien geöffnet lassen, kann jeder auf die Informationen zugreifen oder sogar den Schlüssel für den Zugriff auf die Daten erhalten.

Im Folgenden sind einige Empfehlungen zur Wahrung der optimalen Sicherheit aufgeführt:

- Deaktivieren Sie PGP Virtual Disk-Laufwerke, bevor Sie sich vom Computer entfernen. Die Dateien werden dann sicher in der verschlüsselten Datei gespeichert, die dem Laufwerk zugeordnet ist, bis Sie erneut darauf zugreifen möchten.
- Verwenden Sie einen Bildschirmschoner mit Kennwortschutz, um anderen Personen den Zugriff auf den Computer oder das Anzeigen des Bildschirms zu erschweren, wenn Sie sich nicht am Schreibtisch befinden.
- Stellen Sie sicher, dass die PGP Virtual Disk-Laufwerke nicht für andere Computer im Netzwerk freigegeben werden. Wenden Sie sich dazu ggf. an den Netzwerkadministrator. Die Dateien in einem aktivierten PGP Virtual Disk-Laufwerk sind für alle Personen zugänglich, die sie im Netzwerk sehen können.
- Schreiben Sie Ihre Passphrasen auf keinen Fall auf. Wählen Sie eine Passphrase, die Sie sich merken können. Wenn Sie sich die Passphrase nur schwer merken können, verwenden Sie eine Gedächtnisstütze (z. B. Poster, Lieder, Gedichte oder Witze), aber *schreiben Sie die Passphrasen nicht auf*.
- Wenn Sie PGP Desktop zu Hause einsetzen und den Computer gemeinsam mit anderen Personen verwenden, können diese wahrscheinlich Ihre PGP Virtual Disk-Laufwerksdateien sehen. Deaktivieren Sie daher die nicht benötigten PGP Virtual Disk-Laufwerke, damit ihr Inhalt nicht von anderen Personen gelesen werden kann.

- Wenn eine andere Person physisch Zugriff auf Ihren Computer hat, kann diese Person Ihre PGP Virtual Disk-Laufwerksdateien sowie andere Dateien oder Laufwerke löschen. Wenn der physische Zugriff ein Problem darstellt, sichern Sie die PGP Virtual Disk-Laufwerksdateien oder speichern Sie sie auf einem externen Gerät, auf das nur Sie Zugriff haben.
- Beachten Sie, dass die Kopien des PGP Virtual Disk-Laufwerks denselben Verschlüsselungsschlüssel verwenden wie das Original. Wenn Sie eine Kopie des Laufwerks mit einer anderen Person austauschen und Sie beide Ihre Hauptkennwörter ändern, wird weiterhin derselbe Schlüssel zur Verschlüsselung der Daten verwendet. Der Schlüssel kann dann zwar wiederhergestellt werden, dies ist jedoch nicht einfach.

  Sie können den zugrunde liegenden Schlüssel durch Umschlüsselung des Laufwerks ändern.

13 Mit PGP Portable auf mobile Daten zugreifen

Mit PGP Portable können Sie verschlüsselte Dateien an Benutzer weitergeben, die nicht über PGP Desktop verfügen. Verwenden Sie PGP Portable, um Dateien sicher an andere Systeme weiterzugeben, auf denen keine PGP-Software installiert ist oder installiert werden kann.

PGP Portable bietet folgende Vorteile:

- Transportierbarkeit gesicherter Dokumente
- Einfache Verteilung gesicherter Dokumente

PGP Portable wird von zwei Arten von Benutzern verwendet: von dem Benutzer, der das PGP Portable-Laufwerk mit den gesicherten Daten erstellt, und von dem Benutzer, der nicht über PGP-Software verfügt, aber auf die gesicherten Daten zugreifen muss. Sie können auch zu beiden Arten von Benutzern gehören. Dies wäre beispielsweise der Fall, wenn Sie ein PGP Portable-Laufwerk erstellen, das Sie zu einem Kunden mitnehmen und dort auf einem Computer verwenden.

Unter Mac OS X können Sie auf verschlüsselte Daten *zugreifen*, die auf einem PGP Portable-Laufwerk gespeichert sind.

In diesem Kapitel

Auf Daten auf einem PGP Portable-Laufwerk zugreifen.....203

Auf Daten auf einem PGP Portable-Laufwerk zugreifen

Es gibt drei Möglichkeiten, auf den Inhalt eines PGP Portable-Laufwerks zuzugreifen:

- Durch Aktivieren der CD, DVD bzw. des USB-Wechseldatenträgers unter Windows und Ausführen von PGP Portable (die Anwendung wird bei aktivierter Autorun-Funktion automatisch gestartet).
- Durch Aktivieren der CD, DVD bzw. des USB-Wechseldatenträgers unter Mac OS X und Ausführen von PGP Portable.

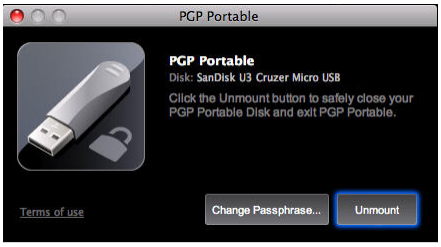
Beachten Sie beim Zugriff auf die Daten auf einem PGP Portable-Laufwerk, dass Sie eigentlich zwei Teile aktivieren: den Wechseldatenträger, auf dem sich das PGP Portable-Laufwerk befindet, und das PGP Portable-Laufwerk (das separat aktiviert wird). Wenn Sie fertig sind, müssen Sie das PGP Portable-Laufwerk deaktivieren, bevor Sie den Wechseldatenträger ordnungsgemäß entfernen.

Die Schritte für den Zugriff auf die Daten auf einem PGP Portable-Laufwerk sind unter Windows und Mac OS X ähnlich.

Warnung: Vergewissern Sie sich, dass Sie einen Wechseldatenträger ordnungsgemäß deaktivieren, bevor Sie ihn physisch vom System entfernen. Andernfalls kann der Dateiinhalt beschädigt werden.

So greifen Sie unter Mac OS X auf Daten auf einem PGP Desktop-Laufwerk zu

1. Legen Sie den Wechseldatenträger ein, auf dem sich das PGP Desktop-Laufwerk befindet. Es kann sich dabei um eine CD/DVD, ein Flash-Laufwerk oder einen anderen Wechseldatenträger handeln.
2. Öffnen Sie den aktivierten Wechseldatenträger und suchen Sie die PGP Desktop-Anwendung (PGP Portable). Doppelklicken Sie auf die Anwendung. Das Dialogfeld „PGP Portable“ wird angezeigt.


PGP Portable
PGP Portable
Disk: SanDisk U3 Cruzer Micro USB
Click the Unmount button to safely close your PGP Portable Disk and exit PGP Portable.
Terms of use
Change Passphrase...
Unmount

3. Geben Sie die Passphrase für das PGP Desktop-Laufwerk ein.

Hinweis: Wenn der Ersteller des PGP Desktop-Laufwerks festgelegt hat, dass die Passphrase bei der ersten Verwendung geändert werden muss, wird beim ersten Anschließen des Laufwerks nach der Erstellung ein Dialogfeld angezeigt, in dem Sie die aktuelle Passphrase eingeben müssen. Zudem werden Sie aufgefordert, die Passphrase zu ändern und die neue Passphrase zu bestätigen.

Nach Eingabe der korrekten Passphrase wird das PGP Desktop-Laufwerk aktiviert. Wenn der Wechseldatenträger mit Lese-/Schreibzugriff aktiviert wurde, können Sie dem PGP Desktop-Laufwerk Daten hinzufügen. Dies ist nicht möglich, wenn das PGP Desktop-Laufwerk als schreibgeschütztes Gerät aktiviert wurde.

Hinweis: Der Laufwerksname für das PGP Desktop-Laufwerk ist für PGP Desktop eindeutig. Er darf nicht mit dem Namen des Laufwerks übereinstimmen.

4 Wenn Sie die Verwendung des PGP Desktop-Laufwerks abgeschlossen haben, deaktivieren Sie das PGP Desktop-Laufwerk (klicken Sie im Dock auf das PGP Desktop-Symbol und dann auf **Deaktivieren**). Das für das PGP Desktop-Laufwerk aktivierte Laufwerk wird deaktiviert.

5 Werfen Sie das USB-Gerät bzw. die CD/DVD ordnungsgemäß aus dem Computer aus.

Warnung: Vergewissern Sie sich, dass Sie einen Wechseldatenträger ordnungsgemäß deaktivieren, bevor Sie ihn physisch vom System entfernen. Andernfalls kann der Dateiinhalt beschädigt werden.

So zeigen Sie verfügbaren Festplattenspeicher an

- Wenn Sie den verfügbaren Festplattenspeicher und die Gesamtgröße des PGP Desktop-Laufwerks nach der Aktivierung des Laufwerks anzeigen möchten, wählen Sie im Dock das PGP Desktop-Symbol aus. Wenn PGP Desktop den freien Speicherplatz noch berechnet, wird die Meldung **Verfügbarer Speicherplatz wird berechnet** angezeigt.

So erhalten Sie zusätzliche Informationen zu PGP Desktop

- Wenn Sie weitere Informationen zu PGP Desktop erhalten möchten, klicken Sie unten links im Dialogfeld **PGP Portable** auf den Link für weitere Informationen. Der Browser wird geöffnet und die Support-Website der PGP Corporation wird angezeigt.

Passphrase für ein PGP Portable-Laufwerk ändern

Gelegentlich kann es erforderlich sein, die mit einem PGP Portable-Laufwerk verknüpfte Passphrase zu ändern. Beachten Sie, dass die Passphrase eines schreibgeschützten PGP Portable-Laufwerks nicht geändert werden kann (dies gilt auch für PGP Portable-Laufwerke, die auf CDs/DVDs gebrannt wurden).

So ändern Sie die Passphrase auf einem PGP Desktop-Laufwerk unter Mac OS X

1 Legen Sie den Wechseldatenträger ein, auf dem sich das PGP Desktop-Laufwerk befindet. Es kann sich dabei um eine CD/DVD, ein Flash-Laufwerk oder einen anderen Wechseldatenträger handeln.

2 Öffnen Sie den Wechseldatenträger und suchen Sie die PGP Desktop-Anwendung (PGP Portable). Doppelklicken Sie auf die Anwendung und geben Sie die Passphrase für das PGP Desktop-Laufwerk ein, wenn Sie dazu aufgefordert werden. Nach Eingabe der korrekten Passphrase wird das PGP Desktop-Laufwerk aktiviert.

3 Öffnen Sie PGP Desktop, indem Sie auf das Symbol im Dock und dann im PGP Desktop-Dialogfeld auf **Passphrase ändern** klicken.

4 Geben Sie die aktuelle Passphrase ein. Geben Sie die neue Passphrase ein, bestätigen Sie diese und klicken Sie auf **Ändern**.

PGP Portable-Laufwerk deaktivieren

Vergewissern Sie sich, dass Sie einen Wechseldatenträger ordnungsgemäß deaktivieren, bevor Sie ihn physisch vom System entfernen. Andernfalls kann der Dateiinhalt beschädigt werden.

So deaktivieren Sie ein PGP Portable-Laufwerk

1 Öffnen Sie PGP Portable. Führen Sie hierzu einen der folgenden Schritte aus:

- Windows: Klicken Sie zum Öffnen von PGP Portable mit der rechten Maustaste auf das Symbol in der Taskleiste und wählen Sie **Deaktivieren und beenden** aus.
- Mac OS: Klicken Sie zum Öffnen von PGP Portable auf das Symbol im Dock und wählen Sie **Deaktivieren und beenden** aus.

Das PGP Portable-Laufwerk wird deaktiviert.

2 Entfernen Sie den Wechseldatenträger vom System.

14 PGP Zip verwenden

Mit PGP Zip können Sie verschlüsselte und komprimierte Pakete, so genannte PGP Zip-Archive, erstellen, öffnen und bearbeiten. In diesem Abschnitt werden die PGP Zip-Funktionen von PGP Desktop erläutert.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat der PGP Universal Server-Administrator möglicherweise bestimmte Funktionen deaktiviert. Wenn eine Funktion deaktiviert wurde, wird das entsprechende Bedienelement auf der linken Seite nicht angezeigt und das Menü und andere Optionen für diese Funktion sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn der PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Übersicht 207
PGP Zip-Archive erstellen 208
PGP Zip-Archive öffnen 210
Signierte PGP Zip-Archive verifizieren 210

Übersicht

Ein PGP Zip-Archiv (Paket) ist eine einzelne Datei, die zur einfachen Datenübertragung und -sicherung komprimiert ist. Diese Archivdateien können eine beliebige Kombination von Dateien und/oder Ordnern enthalten und sind besonders für die Datenübertragung oder Datensicherung geeignet.

Beim Erstellen eines PGP Zip-Archivs können Sie auswählen, ob die Originaldateien nach der Erstellung des Archivs automatisch sicher vom System gelöscht werden sollen. Wenn Sie ein PGP Zip-Archiv erhalten, können Sie entweder alle oder nur bestimmte Dateien und Ordner des Archivs extrahieren.

Sie können folgende Arten von PGP Zip-Archiven erstellen:

- **An einen öffentlichen Schlüssel verschlüsselte Archive**: Wenn Sie das PGP Zip-Archiv an eine oder mehrere Personen senden, über deren öffentliche Schlüssel Sie verfügen, sollten Sie das Archiv an deren öffentliche Schlüssel verschlüsseln, damit nur die gewünschten Empfänger das Archiv öffnen können. Die Empfänger müssen PGP Desktop installiert haben.
- **Mit einer Passphrase verschlüsselte Archive**: Wenn Sie die Verschlüsselung mit einer Passphrase bevorzugen oder das Archiv an mehrere Empfänger senden, deren öffentliche Schlüssel Ihnen nicht bekannt sind, können Sie die konventionelle Verschlüsselung auswählen und das Archiv mit einer Passphrase verschlüsseln. In diesem Fall müssen Sie den Empfängern die Passphrase übermitteln, damit diese das Archiv öffnen können. Die Empfänger müssen PGP Desktop installiert haben.

PGP Zip-Archive werden an den bevorzugten Algorithmus Ihrer Kopie von PGP Desktop (sofern diese von einem PGP-Administrator konfiguriert wurde) oder an AES-256 verschlüsselt. PGP Zip-Archive können frei zwischen Mac OS X- und Windows-Plattformen verschoben werden. PGP Desktop muss auf dem Computer installiert sein, auf den ein PGP Zip-Archiv übertragen werden soll.

PGP Zip-Archive erstellen

So erstellen Sie ein neues PGP Zip-Archiv

1. Öffnen Sie PGP Desktop und klicken Sie auf das Symbol für PGP Zip. Der PGP Zip-Bildschirm wird angezeigt.
2. Klicken Sie auf **Neue PGP Zip-Datei erstellen**. Das Dialogfeld „Unbenanntes PGP Zip-Archiv“ wird angezeigt.
3. Legen Sie auf der Registerkarte **Dateien** fest, welche Dateien und/oder Ordner im PGP Zip-Archiv enthalten sein sollen. Sie haben dazu folgende Möglichkeiten:
   - Ziehen Sie die Dateien bzw. Ordner in die Liste und legen Sie sie dort ab.
   - Klicken Sie auf das Plussymbol unter der Liste und wählen Sie im angezeigten Dialogfeld die Dateien und Ordner aus, die dem PGP Zip-Archiv hinzugefügt werden sollen. Klicken Sie auf **Hinzufügen**, um die Dateien in die Liste einzufügen.

   Wenn Sie eine Datei oder einen Ordner aus der Liste entfernen möchten, wählen Sie die Datei oder den Ordner aus und klicken Sie auf das Minussymbol unter der Liste. Die Datei bzw. der Ordner wird aus der Liste entfernt.

4 Wählen Sie **Originaldateien sicher löschen** aus, wenn Sie die Dateien oder Ordner, die Sie in das PGP Zip-Archiv aufnehmen, sicher vom System löschen möchten.

5 Nachdem Sie die Dateien bzw. Ordner festgelegt haben, die im PGP Zip-Archiv enthalten sein sollen, klicken Sie auf die Registerkarte **Sicherheit**.

6 Geben Sie bei Bedarf einen privaten Schlüssel Ihres Schlüsselbunds an, um dem PGP Zip-Archiv eine **Signatur** hinzuzufügen.

Der angegebene private Schlüssel wird verwendet, um das zu erstellende PGP Zip-Archiv digital zu signieren. Die Empfänger können die Herkunft des Archivs verifizieren, indem sie die digitale Signatur mit dem zugehörigen öffentlichen Schlüssel verifizieren.

- Zeigen Sie die Eigenschaften des ausgewählten Signaturschlüssels an, indem Sie rechts neben der Benutzer-ID des Schlüssels auf das Schlüsselsymbol klicken. Schließen Sie das Dialogfeld „Schlüssel-Info“, wenn Sie fertig sind.

7 Wählen Sie die gewünschte Verschlüsselungsmethode aus:

- **Mit Empfängerschlüsseln verschlüsseln**: Verschlüsselt das PGP Zip-Archiv an die öffentlichen Schlüssel der Empfänger. Dadurch wird sichergestellt, dass nur diese Empfänger das Archiv öffnen können.

  Wenn Sie die Verschlüsselung mit öffentlichen Schlüsseln auswählen, können Sie die öffentlichen Schlüssel der Empfänger in die Liste ziehen und dort ablegen oder auf das Plussymbol klicken und die öffentlichen Schlüssel der gewünschten Empfänger auswählen.

- **Nur mit Passphrase verschlüsseln**: Verschlüsselt das PGP Zip-Archiv mit einer Passphrase, die Sie beim Speichern des Archivs festlegen. Nur Personen, denen die Passphrase bekannt ist, können das Archiv öffnen. Vergessen Sie nicht, den Empfängern die Passphrase mitzuteilen, damit diese das PGP Zip-Archiv öffnen können.

  Geben Sie die Passphrase in das Feld **Passphrase** ein und wiederholen Sie die Eingabe im Feld **Bestätigen**. Wenn die Zeichen während der Eingabe der Passphrase angezeigt werden sollen, wählen Sie **Tastatureingabe anzeigen** aus.

- **Nur signieren (keine Verschlüsselung)**: Erstellt ein nicht verschlüsseltes PGP Zip-Archiv. Da Sie das PGP Zip-Archiv nicht verschlüsseln, müssen Sie jedoch im Feld **Signatur** einen Signaturschlüssel angeben.

8 Wenn das PGP Zip-Archiv nur eine Datei enthält und Sie die Datei signieren, jedoch nicht verschlüsseln, erstellen Sie eine separate Signaturdatei, indem Sie das Kontrollkästchen **Separate Signaturdatei speichern** aktivieren.

Wenn Sie eine separate Signaturdatei erstellen möchten, können Sie *nur eine* Datei in das Archiv aufnehmen und müssen einen Signaturschlüssel auswählen. Das Archiv kann nicht verschlüsselt werden.

9 Klicken Sie auf **Speichern**.

10 Geben Sie einen Dateinamen und einen Speicherort für das PGP Zip-Archiv an und klicken Sie auf **Speichern**. Falls Sie im Feld **Signatur** einen Signaturschlüssel angegeben haben, werden Sie zur Eingabe der Passphrase des Signaturschlüssels aufgefordert (sofern diese nicht zwischengespeichert wurde).

11 Geben Sie die Passphrase ein und klicken Sie auf **OK**. Das PGP Zip-Archiv wird am angegebenen Speicherort erstellt.

PGP Zip-Archive öffnen

PGP Desktop muss auf dem Computer installiert sein, damit ein PGP Zip-Archiv geöffnet werden kann.

So öffnen Sie ein PGP Zip-Archiv

1 Doppelklicken Sie auf die Archivdatei und führen Sie einen der folgenden Schritte aus:

- Wenn das Archiv an Ihren öffentlichen Schlüssel verschlüsselt wurde, werden Sie zur Eingabe der Passphrase Ihres privaten Schlüssels aufgefordert. Diese wird dann zum Entschlüsseln des Archivs verwendet. (Falls die Passphrase zwischengespeichert wurde, müssen Sie sie nicht erneut eingeben.) Geben Sie die entsprechende Passphrase ein und klicken Sie auf **OK**.
- Wenn das Archiv an eine Passphrase verschlüsselt wurde, werden Sie zur Eingabe der Passphrase aufgefordert. Geben Sie die entsprechende Passphrase ein und klicken Sie auf **OK**.

Wenn das Archiv zusätzlich signiert wurde, versucht PGP Desktop, die Signatur zu verifizieren. Anschließend wird ein Bildschirm mit dem Ergebnis der Verifizierung angezeigt.

2 Wenn das Archiv zwei oder mehr Dateien bzw. Ordner enthält, wird ein neuer Ordner für die Dateien und/oder Ordner aus dem PGP Zip-Archiv erstellt.

Enthält das Archiv nur eine Datei, wird nur diese Datei am Speicherort des PGP Zip-Archivs erstellt.

Signierte PGP Zip-Archive verifizieren

Wenn Sie ein **signiertes PGP Zip-Archiv erhalten haben, sollten Sie es verifizieren, um den Absender zu ermitteln und sicherzustellen, dass das Archiv nicht verfälscht wurde, bevor es zu Ihnen gelangt ist. Nicht signierte Dateien können nicht verifiziert werden.**

So verifizieren Sie ein signiertes PGP Zip-Archiv

1. Klicken Sie in PGP Desktop auf **Ansicht > Verifizierungsinformationen**. Der Bildschirm „Verifizierungsinformationen“ wird angezeigt.
2. Ziehen Sie die signierte PGP Zip-Datei (.pgp), die Sie verifizieren möchten, in das Feld **Signierte Dateien hier ablegen**. PGP Desktop verifiziert die Signatur und zeigt die Verifizierungsinformationen an.
3. Wenn Sie die Liste der verifizierten Archive löschen möchten, klicken Sie auf **Löschen**. Alle Einträge im Bildschirm „Verifizierungsinformationen“ werden entfernt.

15 Dateien mit PGP Shredder sicher löschen

Falls Sie vertrauliche Dateien vollständig vernichten möchten, ohne Fragmente der Daten zurückzulassen, verwenden Sie das Dienstprogramm PGP Shredder.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat der PGP Universal Server-Administrator möglicherweise bestimmte Funktionen deaktiviert. Wenn eine Funktion deaktiviert wurde, wird das entsprechende Bedienelement auf der linken Seite nicht angezeigt und das Menü und andere Optionen für diese Funktion sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn der PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Dateien und Ordner mit PGP Shredder sicher und endgültig löschen .. 213

Dateien und Ordner mit PGP Shredder sicher und endgültig löschen

Wenn Sie vertrauliche Dateien oder Ordner vollständig vernichten möchten, verwenden Sie hierzu PGP Shredder. Wenn Sie Dateien oder Ordner mit PGP Shredder löschen, bleiben keine Spuren zurück.

PGP Shredder überschreibt die Daten mit Zufallstext. Dieser Vorgang wird in mehreren *Durchgängen* ausgeführt. Sie können die Anzahl der Durchgänge der PGP Shredder-Funktion festlegen, indem Sie im Bildschirm „Einstellungen“ den Bereich „Laufwerk“ öffnen. Weitere Informationen zum Einstellen von Optionen und Einstellungen finden Sie im Abschnitt zu Laufwerksoptionen und -einstellungen unter *Laufwerksoptionen* (siehe "*Laufwerkseinstellungen*" auf Seite 228).

Das sichere Löschen kann einige Zeit in Anspruch nehmen. Die Dauer hängt u. a. von der Anzahl der festgelegten Durchgänge, der Prozessorgeschwindigkeit sowie der Anzahl der ausgeführten anderen Anwendungen ab.

Hinweis: Bei drei Durchgängen überschreitet PGP Shredder bereits die Mindestvorschriften der Datenträgerrichtlinien des US-Verteidigungsministeriums, Norm 5220.22-M. Obwohl eine größere Anzahl von Durchgängen zulässig ist, sind für moderne Diskhardware nicht mehr als zwei Durchgänge erforderlich. Die Sicherheit erhöht sich weiter bis zu ungefähr 28 Durchgängen. Mit PGP Shredder können bis zu 49 Durchgänge ausgeführt werden, jedoch ist dabei zu beachten, dass der erforderliche Zeitaufwand mit der Anzahl der Durchgänge zunimmt.

PGP Shredder kann auf verschiedene Weise eingesetzt werden:

- Verwenden Sie das PGP Shredder-Symbol. Bei der Installation von PGP Desktop wurde PGP Shredder im gleichen Verzeichnis wie PGP Desktop installiert. Wenn Sie ein Alias für PGP Shredder erstellen und dieses im Dock oder auf dem Schreibtisch ablegen, können Sie PGP Shredder einfach und bequem nutzen.
- Verwenden Sie das PGP Shredder-Symbol in der PGP-Symbolleiste. Klicken Sie auf das PGP Shredder-Symbol in der Symbolleiste und suchen Sie dann nach den Dateien oder Ordnern, die Sie sicher löschen möchten.
- Wählen Sie **Datei > Sicher löschen** aus, und wechseln Sie zu den Dateien oder Ordnern, die Sie sicher löschen möchten.
- Verwenden Sie die Kontextmenüs im Finder. Drücken Sie die Ctrl-Taste und klicken Sie auf die Datei oder den Ordner oder klicken Sie bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste auf die Datei oder den Ordner. Wählen Sie **PGP > Sicher löschen** aus.

Achtung: Einige Dateisysteme nutzen eine als Journalerstellung bezeichnete Funktion. Die Funktion wurde von Apple für Mac OS Extended-Dateisysteme (HFS+) in Mac OS X 10.2.2. eingeführt. Bei der Journalerstellung werden alle Daten, die auf die Festplatte geschrieben werden, in Form einer zusätzlichen Kopie in einem privaten Bereich des Dateisystems abgelegt. Dadurch werden beim sicheren Löschen der Originaldatei deren Daten in einen anderen Bereich der Festplatte geschrieben. Vermeiden Sie dieses Problem, indem Sie die *Journalerstellung nicht verwenden*. Die Journalerstellung kann über das Festplattendienstprogramm von Apple deaktiviert werden. Weitere Informationen zur Dateisystem-Journalerstellung finden Sie im technischen Artikel des Apple-Supports *Apple Support Technical Article 107249* (*http://docs.info.apple.com/article.html?artnum=107249*).

Tipp: Viele Anwendungen speichern automatisch Dateien, die in Bearbeitung sind. Daher können Sicherungskopien der gelöschten Dateien vorhanden sein. Nachdem Sie die primäre Kopie einer Datei gelöscht haben, empfiehlt die PGP Corporation, sämtliche Sicherungskopien mit PGP Shredder sicher zu löschen.

Dateien über das PGP Shredder-Symbol sicher löschen

▸ **So werden Dateien oder Ordner über das PGP Shredder-Symbol sicher gelöscht**

1. Wechseln Sie zu den Dateien oder Ordnern, die Sie sicher löschen möchten.
2. Ziehen Sie die Dateien und Ordner auf das PGP Shredder-Symbol. Sie werden in einem Bestätigungsdialogfeld aufgefordert, das sichere Löschen der aufgeführten Dateien und/oder Ordner zu bestätigen.
3. Klicken Sie auf **OK**. Die Dateien bzw. Ordner werden sicher vom System gelöscht.

Tipp: Erstellen Sie ein Alias für das PGP Shredder-Symbol auf dem Desktop, damit Sie Dateien über dieses Symbol sicher löschen können, ohne auf den Anwendungsordner zugreifen zu müssen. Ziehen Sie das Alias dann auf den Schreibtisch (oder ins Dock).

Dateien über das Symbol „Dateien sicher löschen“ in der Symbolleiste von PGP Desktop sicher löschen

▸ **So werden Dateien oder Ordner über die Symbolleiste von PGP Desktop sicher gelöscht**

1. Klicken Sie in der Symbolleiste auf das Symbol **Dateien sicher löschen**.
2. Wählen Sie die Dateien oder Ordner aus, die Sie sicher löschen möchten, und klicken Sie auf **Sicher löschen**. Sie werden in einem Bestätigungsdialogfeld aufgefordert, das sichere Löschen der aufgeführten Dateien und/oder Ordner zu bestätigen.
3. Klicken Sie auf **OK**. Die Dateien bzw. Ordner werden sicher vom System gelöscht.

Dateien über den Befehl „Sicher löschen“ im Menü „Datei“ sicher löschen

▸ **So werden Dateien oder Ordner über den Befehl „Sicher löschen“ sicher gelöscht**

1. Klicken Sie auf **Datei > Sicher löschen**.

2 Wählen Sie die Dateien oder Ordner aus, die Sie sicher löschen möchten, und klicken Sie auf **Sicher löschen**. Sie werden in einem Bestätigungsdialogfeld aufgefordert, das sichere Löschen der aufgeführten Dateien und/oder Ordner zu bestätigen.

3 Klicken Sie auf **OK**. Die Dateien bzw. Ordner werden sicher vom System gelöscht.

Dateien im Finder sicher löschen

▸ **So werden Dateien oder Ordner im Finder sicher gelöscht**

1 Wählen Sie im Finder die Dateien oder Ordner aus, die Sie sicher löschen möchten.

2 Halten Sie die Ctrl-Taste gedrückt und klicken Sie auf eine Datei oder einen Ordner (bzw. klicken Sie bei Verwendung einer Maus mit zwei Tasten mit der rechten Maustaste darauf). Wählen Sie **PGP > Sicher löschen** aus. Sie werden in einem Bestätigungsdialogfeld aufgefordert, das sichere Löschen der aufgeführten Dateien und/oder Ordner zu bestätigen.

3 Klicken Sie auf **OK**. Die Dateien bzw. Ordner werden sicher vom System gelöscht.

16 PGP Desktop-Einstellungen festlegen

PGP Desktop ist auf die Anforderungen der meisten Benutzer zugeschnitten. Sie können jedoch einige Einstellungen an Ihre spezifischen Anforderungen anpassen. In diesem Abschnitt werden die Optionen und ihre Einstellungsmöglichkeiten in PGP Desktop erläutert.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung verwenden, hat der PGP Universal Server-Administrator möglicherweise bestimmte Funktionen deaktiviert. Wenn eine Funktion deaktiviert wurde, wird das entsprechende Bedienelement auf der linken Seite nicht angezeigt und das Menü und andere Optionen für diese Funktion sind nicht verfügbar. Die in diesem Handbuch enthaltenen Abbildungen entsprechen der Standardinstallation, bei der alle Funktionen aktiviert sind. Wenn der PGP Universal Server-Administrator diese Funktion deaktiviert hat, ist dieser Abschnitt für Sie nicht relevant.

In diesem Kapitel

Auf PGP Desktop-Einstellungen zugreifen 217
Allgemeine Einstellungen 218
Schlüsseleinstellungen 220
Hauptschlüsseleinstellungen 222
Messaging-Einstellungen 223
Laufwerkseinstellungen 228
Benachrichtigungseinstellungen 229
Erweiterte Einstellungen 232

Auf PGP Desktop-Einstellungen zugreifen

So greifen Sie auf die PGP Desktop-Einstellungen zu

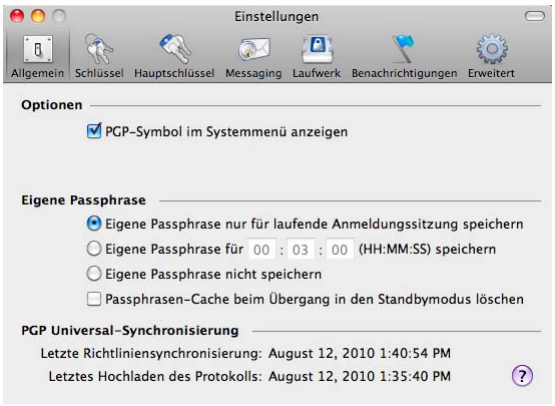
1. Öffnen Sie PGP Desktop.
2. Klicken Sie auf **PGP > Einstellungen**.

- Wechseln Sie zwischen den verschiedenen Einstellungsbereichen, indem Sie auf die Symbole im oberen Bereich des Dialogfelds **Einstellungen** klicken.

3 Wenn Sie alle Einstellungen festgelegt haben, klicken Sie auf das Schließen-Symbol (den roten Kreis oben links im Bildschirm).

Allgemeine Einstellungen

In den allgemeinen Einstellungen sind verschiedene PGP Desktop-Einstellungen verfügbar.



Die Registerkarte „Allgemein“ des Dialogfelds „Einstellungen“ weist folgende Optionen auf:

- **PGP-Symbol im Systemmenü anzeigen:** Wenn diese Option aktiviert ist, wird das PGP Desktop-Symbol in der Menüleiste von Mac OS X angezeigt, während PGP Desktop im System aktiv ist. Über das PGP-Symbol in der Menüleiste können Sie problemlos auf Funktionen von PGP Desktop zugreifen.
  - Wenn Sie das PGP Desktop-Symbol aus der Menüleiste entfernen möchten, deaktivieren Sie das Kontrollkästchen.
  - Stellen Sie das PGP Desktop-Symbol in der Menüleiste wieder her, indem Sie in den allgemeinen Einstellungen das Kontrollkästchen **PGP-Symbol im Systemmenü anzeigen** aktivieren.

  Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist diese Option möglicherweise erforderlich.

  Durch das Entfernen des PGP Desktop-Symbols aus der Menüleiste werden die PGP Desktop-Dienste *nicht* angehalten, sondern weiterhin ausgeführt.

- Wenn die PGP Desktop-Dienste angehalten werden sollen, drücken Sie die **Wahltaste**. Klicken Sie in der Menüleiste auf das PGP Desktop-Symbol und wählen Sie **Beenden** aus.

Hinweis: Die PGP Corporation empfiehlt, die PGP Desktop-Dienste nur bei Bedarf anzuhalten.

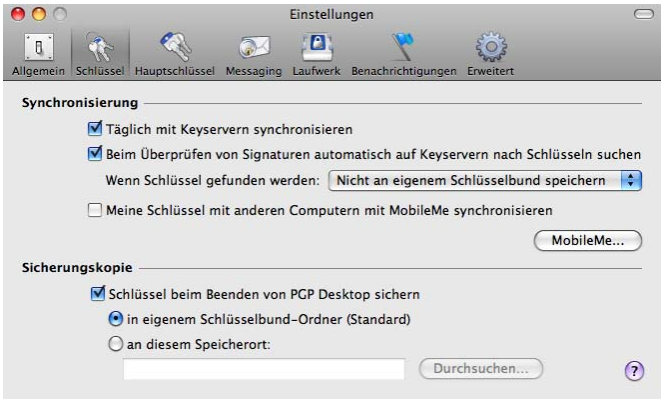
- **Eigene Passphrase**: Bietet Optionen zum Speichern der Passphrase.
  - **Eigene Passphrase nur für laufende Anmeldungssitzung speichern**: Speichert die Passphrase automatisch, bis Sie sich vom Computer abmelden. Dieser Vorgang wird als *Zwischenspeicherung* der Passphrase bezeichnet. Wenn diese Option aktiviert ist, werden Sie für jeden privaten Schlüssel einmal zur Eingabe der Passphrase aufgefordert. Sie müssen die Passphrase bis zum Abmelden vom Computer nicht erneut für den Schlüssel eingeben.

Achtung: Wenn diese Option aktiviert ist, ist es äußerst wichtig, dass Sie sich vom Computer abmelden, bevor Sie ihn verlassen. (Sie können sich abmelden, indem Sie im Apple-Menü die Option **[Ihr Name] abmelden** auswählen.) Falls Sie sich nie abmelden, kann die Passphrase wochenlang zwischengespeichert bleiben. Unbefugte Personen können in diesem Fall Ihre verschlüsselten Nachrichten lesen oder Nachrichten mit Ihrem Schlüssel verschlüsseln, wenn Sie sich nicht am Computer befinden. Wenn Sie in der Regel für längere Zeit am Computer angemeldet sind, wählen Sie eine der anderen Zwischenspeicherungsoptionen.

  - **Eigene Passphrase für X speichern**: Speichert die Passphrase für den angegebenen Zeitraum automatisch im Speicher. Wenn Sie diese Option aktivieren, werden Sie einmal für die erste Signierungs- oder Entschlüsselungsaufgabe zur Eingabe der Passphrase aufgefordert. Sie werden während des festgelegten Zeitraums nicht erneut zur Eingabe der Passphrase aufgefordert. Der Zeitraum wird mithilfe der Felder für **Stunden, Minuten und Sekunden** festgelegt. Die Standardeinstellung beträgt zwei Minuten.
  - **Eigene Passphrase nicht speichern**: Verhindert, dass die Passphrase im Speicher abgelegt wird. Wenn Sie diese Option aktivieren, müssen Sie die Passphrase immer eingeben, wenn sie benötigt wird.
  - **Passphrasen-Cache beim Übergang in den Standbymodus löschen**: Ist diese Einstellung aktiviert, löscht PGP Desktop alle Passphrasen im Speicher, wenn der Computer in den Standbymodus wechselt. (Nicht alle Computer verfügen über einen Standbymodus.)
- **PGP Universal-Synchronisierung:** Wenn Sie eine von einem PGP Universal Server verwaltete Umgebung verwenden, werden in diesem Feld Informationen zur letzten Richtlinienaktualisierung und zum letzten Senden der Protokolle angezeigt.

Schlüsseleinstellungen

Das Dialogfeld „Schlüssel“ enthält Einstellungen für PGP Desktop-Schlüssel.



Folgende Optionen sind verfügbar:

- **Synchronisierung**: Mit diesen Einstellungen wird festgelegt, wie Schlüssel auf Schlüsselbunden mit den öffentlichen Servern synchronisiert werden.
  - **Täglich mit Keyservern synchronisieren**: Wenn diese Option ausgewählt ist, führt PGP Desktop täglich eine Synchronisierung der öffentlichen Schlüssel am Schlüsselbund mit der Liste der Keyserver durch. Diese Liste enthält auch das PGP Global Directory.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, ist diese Option möglicherweise erforderlich.

Sind geänderte Versionen der Schlüssel verfügbar, werden sie automatisch heruntergeladen. Wenn PGP Desktop vom Keyserver benachrichtigt wird, dass ein Schlüssel vom Keyserver entfernt wurde, deaktiviert PGP Desktop diesen Schlüssel am lokalen Schlüsselbund.

Wenn Sie mit PGP Desktop eine Änderung an einem öffentlichen Schlüssel am Schlüsselbund vornehmen, wird diese Änderung nicht automatisch vom Computer auf den Keyserver hochgeladen. Sie müssen den geänderten Schlüssel manuell auf den gewünschten Keyserver hochladen. Wenn Sie PGP Desktop beenden, werden Sie zum Hochladen geänderter Schüssel aufgefordert. Sie können den Schlüssel jedoch auch an den Keyserver senden, indem Sie mit der rechten Maustaste auf den geänderten Schlüssel klicken, aus dem Kontextmenü die Option zum Senden auswählen **und dann in der Liste auf den gewünschten Keyserver klicken.**

- **Beim Überprüfen von Signaturen automatisch auf Keyservern nach Schlüsseln suchen:** Mit dieser Option können Sie festlegen, dass PGP Desktop automatisch auf den konfigurierten Keyservern nach dem erforderlichen öffentlichen Schlüssel sucht, wenn Sie eine E-Mail-Nachricht erhalten, die mit einem privaten Schlüssel signiert wurde, dessen entsprechender öffentlicher Schlüssel sich *nicht* am lokalen Schlüsselbund befindet.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, wird diese Option nicht verwendet. Der PGP Universal Server definiert, ob Schlüssel gesucht und, wenn gefunden, zwischengespeichert werden. Schlüssel, die in einer von einem PGP Universal Server verwalteten Umgebung gefunden werden, werden nie am Schlüsselbund gespeichert.

- **Wenn Schlüssel gefunden werden**: Wenn der öffentliche Schlüssel auf dem Keyserver gefunden *wird*, gibt es drei Optionen:
  - **Nicht an eigenem Schlüsselbund speichern:** Alle auf den konfigurierten Keyservern gefundenen Schlüssel werden nur einmal verwendet, um die Signatur zu überprüfen, mit der Sie gegenwärtig arbeiten. Der Schlüssel wird nicht am Schlüsselbund gespeichert.
  - **Zum Speichern an eigenem Schlüsselbund auffordern:** Diese Option legt fest, dass PGP Desktop eine Aufforderung anzeigt, ob Sie die gefundenen Schlüssel am lokalen Schlüsselbund speichern möchten.
  - **Schlüssel an eigenem Schlüsselbund speichern**: Mit dieser Option legen Sie fest, dass gefundene Schlüssel automatisch am lokalen Schlüsselbund gespeichert werden.

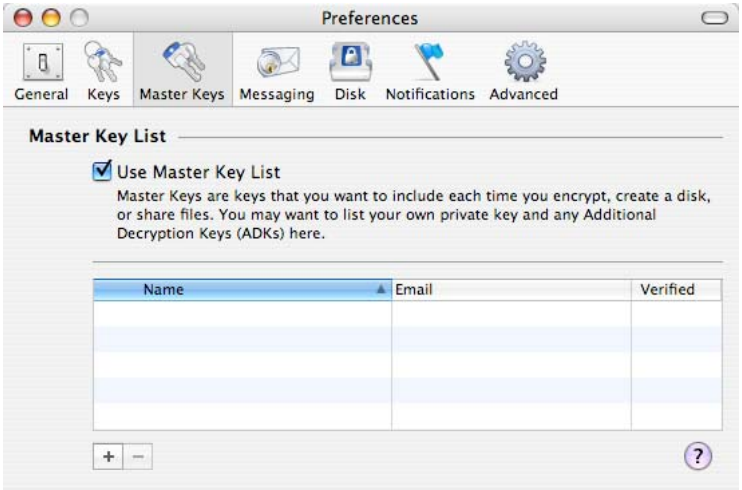
  Diese Optionen finden auch auf in S/MIME-E-Mail-Nachrichten enthaltene X.509-Zertifikate Anwendung. Wenn dies entsprechend angegeben ist, extrahiert PGP Desktop das X.509-Zertifikat und importiert es dann an den Schlüsselbund. Wenn Sie E-Mail-Nachrichten mit importierten Zertifikaten verschlüsseln möchten, müssen Sie das Zertifikat manuell signieren.
- **Meine Schlüssel mit anderen Computern mit MobileMe synchronisieren**: (MobileMe ist die neue .Mac-Version von Apple.) Aktivieren Sie dieses Kontrollkästchen, wenn Sie Ihre Schlüssel mit Ihrem MobileMe-Konto synchronisieren möchten. (Sie benötigen ein entsprechendes Konto, um diese Option zu verwenden.) Wenn die Option ausgewählt ist, kopiert die Synchronisierungs-Engine die Schlüsseldateien in einen lokalen Zwischenspeicher, der von MobileMe zur Aktualisierung verwendet wird.

- Klicken Sie auf **MobileMe**, wenn Sie die Schlüssel sofort mit dem MobileMe-Konto synchronisieren möchten. Das MobileMe-Fenster der Systemeinstellungen wird angezeigt. Melden Sie sich an, klicken Sie in den Synchronisierungsbereich, wählen Sie aus der Liste das Element „PGP Keys“ aus und klicken Sie auf **Jetzt synchronisieren**.

- **Sicherungskopie**: Mit diesen Einstellungen wird festgelegt, wann und wo die Schlüssel gesichert werden sollen.
  - **Schlüssel beim Beenden von PGP Desktop sichern**: Wenn diese Option aktiviert ist, sichert PGP Desktop die Schlüssel automatisch am angegebenen Speicherort:
    - **In eigenem Schlüsselbund-Ordner (Standard):** Wenn diese Option ausgewählt ist, werden die Schlüssel im standardmäßigen Schlüsselbundordner auf dem System gesichert.
    - **An diesem Speicherort:** Wenn diese Option ausgewählt ist, werden die Schlüssel an einem von Ihnen festgelegten Speicherort auf dem Computer gesichert. Klicken Sie auf **Durchsuchen**, um einen Speicherort anzugeben.

Hauptschlüsseleinstellungen

Die Hauptschlüsselliste enthält eine Reihe von Schlüsseln, die Sie standardmäßig jedes Mal hinzufügen möchten, wenn Sie Schlüssel für Messaging, Laufwerksverschlüsselung oder PGP Zip auswählen. Die betreffenden Schlüssel müssen in diesem Fall nicht mehr in das Feld **Empfänger** gezogen werden.

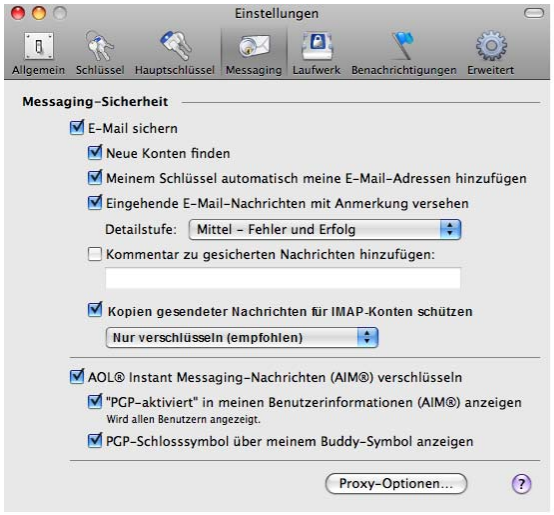


Wenn Sie die Hauptschlüsselliste verwenden möchten, aktivieren Sie das Kontrollkästchen **Hauptschlüssellisteverwenden. Sie können nur Schlüssel in die Hauptschlüsselliste aufnehmen bzw. daraus entfernen, wenn dieses Kontrollkästchen aktiviert ist.**

Hinweis: Wenn Sie Ihren Schlüssel mithilfe des Einrichtungsassistenten erstellt haben, wird er der Hauptschlüsselliste automatisch hinzugefügt. Wenn Sie die Schlüsselerstellung übersprungen und den Schlüssel in PGP Desktop importiert haben, wird der Schlüssel nicht automatisch der Liste hinzugefügt.

Messaging-Einstellungen

Mit den Einstellungen im Bereich **Messaging** wird die Messaging-Sicherheit konfiguriert. Darüber hinaus können Sie auf Einstellungen für E-Mail und Instant Messaging zugreifen.



Im Bereich **Messaging** sind folgende Einstellungen verfügbar:

- **E-Mail sichern:** Aktivieren Sie das Kontrollkästchen **E-Mail sichern**, wenn Ihre gesamten E-Mail-Konten automatisch von PGP Desktop gesichert werden sollen. Wenn diese Option aktiviert ist, fängt PGP Desktop alle eingehenden und ausgehenden E-Mail-Nachrichten ab und sichert sie entsprechend der jeweiligen Richtlinien.

  Deaktivieren Sie das Kontrollkästchen **E-Mail sichern**, wenn Ihre E-Mail-Konten nicht mehr von PGP Desktop gesichert werden sollen.

Wenn Sie das Kontrollkästchen **E-Mail sichern** aktivieren, können Sie zusätzlich folgende Optionen auswählen:

- **Neue Konten finden:** Aktivieren Sie dieses Kontrollkästchen, wenn PGP Desktop Ihre E-Mail-Aktivitäten überwachen und automatisch nach neuen, von Ihnen verwendeten E-Mail-Konten suchen soll. Die über die erkannten Konten gesendeten Nachrichten werden dann ebenfalls gesichert.

Hinweis: Wenn Sie PGP Desktop in einer von PGP Universal verwalteten Umgebung einsetzen, unterbindet die Verwendung einer Platzhalterbindung (*) diese Funktion, da alle Maildienste der Platzhalterbindung * entsprechen. Daher entsprechen alle neuen Konten automatisch den Richtlinien und werden erstellt, auch wenn diese Option deaktiviert ist.

- **Meinem Schlüssel automatisch meine E-Mail-Adressen hinzufügen:** Wenn Sie dieses Kontrollkästchen aktivieren, fügt PGP Desktop Ihrem Schlüssel automatisch die zum Senden von Nachrichten verwendeten E-Mail-Adressen hinzu. Diese Option ist standardmäßig aktiviert.

  Deaktivieren Sie dieses Kontrollkästchen, damit E-Mail-Adressen dem Schlüssel nicht automatisch hinzugefügt werden. Dies dient dem Datenschutz. Sie können dadurch beispielsweise verhindern, dass jemand Ihre E-Mail-Adresse ermittelt.

- **Eingehende E-Mail-Nachrichten mit Anmerkung versehen:** Aktivieren Sie dieses Kontrollkästchen, wenn eingehende E-Mail-Nachrichten mit Anmerkungen versehen werden sollen, in denen die von PGP Desktop durchgeführten Verarbeitungsschritte beschrieben werden. Sie können zwischen drei Anmerkungsstufen wählen:

  - **Maximal: Ausführliche Anmerkung:** In den Anmerkungen wird jede Aktion beschrieben, die von PGP Desktop während der Verarbeitung durchgeführt wurde.
  - **Mittel: Fehler und Erfolg**: Dies ist die Standardoption. Es werden Anmerkungen hinzugefügt, wenn Verarbeitungsprobleme aufgetreten sind, z. B. unbekannte Schlüssel oder Signierer. Bei der Einstellung „Mittel“ werden allen entschlüsselten und/oder signierten E-Mail-Nachrichten Anmerkungen hinzugefügt, jedoch werden einzelne angehängte Dateien nicht aufgeführt.
  - **Minimal: Nur Fehler:** Es werden nur Anmerkungen hinzugefügt, wenn Verarbeitungsprobleme aufgetreten sind, z. B. unbekannte Schlüssel oder Signierer.

- **Kommentar zu gesicherten Nachrichten hinzufügen:** Wenn diese Option aktiviert ist, wird der hier eingegebene Text stets in verschlüsselte oder signierte Nachrichten aufgenommen. In dieses Feld eingegebene Kommentare werden in jeder gesicherten Nachricht unterhalb der Textkopfzeile `--BEGIN PGP MESSAGE BLOCK--` und der Versionsnummer von PGP Desktop angezeigt. Diese Kommentare werden in entschlüsselten E-Mail-Nachrichten nicht angezeigt.

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, enthält dieses Feld möglicherweise bereits Text.

- **Kopien gesendeter Nachrichten für IMAP-Konten schützen**: Diese Option steht nur bei eigenständigen Installationen zur Verfügung. Aktivieren Sie dieses Kontrollkästchen, wenn Sie E-Mail-Nachrichten schützen möchten, wenn sie in den IMAP-Ordner für gesendete Objekte kopiert werden. Diese Option bietet zusätzliche Sicherheit, damit Sie vertrauliche E-Mail-Nachrichten schützen können, die Sie über das IMAP-Konto gesendet haben.

  Wenn Sie diese Option auswählen, müssen Sie auch auswählen, wie die Kopien der gesendeten Nachrichten gesichert werden sollen:

  - **Nur verschlüsseln (empfohlen)**: Dies ist die Standardoption. Wählen Sie diese Option aus, um Nachrichten zu verschlüsseln, wenn sie in den Ordner für gesendete Objekte kopiert werden.
  - **Verschlüsseln und signieren**: Wählen Sie diese Option aus, um Nachrichten zu verschlüsseln und zu signieren, wenn sie in den Ordner für gesendete Objekte kopiert werden.
  - **Nur signieren**: Wählen Sie diese Option aus, um Nachrichten zu signieren (und nicht zu verschlüsseln), wenn sie in den Ordner für gesendete Objekte kopiert werden.

  Wenn der Name des Ordners nicht von PGP Desktop erkannt wird (wenn der Ordner beispielsweise nicht „Gesendete Objekte“, sondern „Ausgehende Nachrichten“ heißt), werden Sie in einer Meldung gefragt, ob Ihre gesendeten Nachrichten gewöhnlich in diesem Ordner gespeichert werden. Beachten Sie, dass die erste in diesen Ordner kopierte Nachricht nicht verschlüsselt und/oder signiert ist. Nachfolgend in diesen Ordner kopierte Nachrichten werden jedoch verschlüsselt und/oder signiert.

- **AOL® Instant Messaging-Nachrichten (AIM®) verschlüsseln:** Aktivieren Sie diese Option, wenn PGP Desktop Instant Messaging-Sitzungen mit kompatiblen Instant Messaging-Clients verschlüsseln soll. Der andere Teilnehmer der IM-Sitzung muss ebenfalls PGP Desktop verwenden.

  AOL® Instant Messenger™ und iChat-Softwareanwendungen sind kompatibel.

- **„PGP-aktiviert“ in meinen Benutzerinformationen (AIM) anzeigen**: Wenn diese Option aktiviert ist, wird der Hinweis **PGP-aktiviert** zusammen mit Ihrem Benutzernamen z. B. in der AIM-Buddy-Liste oder im Befehl zum Abrufen von Buddy-Informationen angezeigt. Ist die Option deaktiviert, wird Ihr Benutzername ohne diesen Hinweis angezeigt. **Das Erscheinungsbild dieses Textes kann abhängig vom jeweiligen Instant Messaging-Client variieren.**
- **PGP-Schlosssymbol über meinem Buddy-Symbol anzeigen**: Wenn diese Option aktiviert ist, wird das stilisierte PGP-Schlosssymbol über Ihrem Buddy-Symbol angezeigt. Andere Benutzer erkennen daran, dass die Instant Messaging-Sitzung geschützt ist. Ist die Option deaktiviert, wird Ihr Symbol normal angezeigt.

- Klicken Sie auf die Schaltfläche **Proxy-Optionen**, um auf erweiterte Messaging-Einstellungen zuzugreifen.

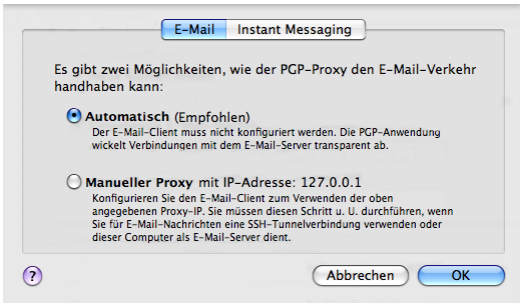
Proxy-Optionen

Klicken Sie auf **Proxy-Optionen**, um erweiterte E-Mail- und IM-Einstellungen anzuzeigen.

E-Mail-Einstellungen

Verwenden Sie diese Option, wenn ein Proxy auf dem Computer manuell konfiguriert werden muss, damit Sie E-Mail-Nachrichten senden und empfangen können.

PGP Desktop ist zwischen Ihre E-Mail-Anwendung und den E-Mail-Server geschaltet, der für die Zustellung Ihrer E-Mail-Nachrichten zuständig ist. Dadurch kann PGP Desktop den Nachrichtenverkehr automatisch für Sie filtern bzw. als *Proxy* dienen. Auf diese Weise schützt PGP Desktop Ihre Nachrichten anhand der jeweiligen Richtlinie, ohne Sie bei der Arbeit zu behindern.


E-Mail
Instant Messaging
Es gibt zwei Möglichkeiten, wie der PGP-Proxy den E-Mail-Verkehr handhaben kann:
Automatisch (Empfohlen)
Der E-Mail-Client muss nicht konfiguriert werden. Die PGP-Anwendung wickelt Verbindungen mit dem E-Mail-Server transparent ab.
Manueller Proxy mit IP-Adresse: 127.0.0.1
Konfigurieren Sie den E-Mail-Client zum Verwenden der oben angegebenen Proxy-IP. Sie müssen diesen Schritt u. U. durchführen, wenn Sie für E-Mail-Nachrichten eine SSH-Tunnelverbindung verwenden oder dieser Computer als E-Mail-Server dient.
?
Abbrechen
OK

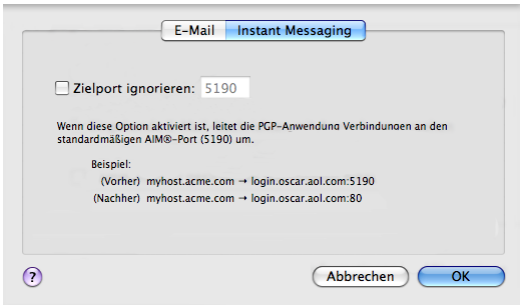
In der Regel müssen Sie die Proxyeinstellungen der PGP-Anwendung nicht ändern. In manchen Situationen müssen die Proxyeinstellungen jedoch manuell festgelegt werden. Verwenden Sie die vom Netzwerkadministrator empfohlene Einstellung:

- **Automatisch:** Die empfohlene Standardeinstellung. Ihre E-Mail-Nachrichten werden automatisch und transparent geschützt. Die PGP Corporation empfiehlt, diese Option ausgewählt zu lassen, sofern Sie nicht zur Verwendung der manuellen Proxyeinstellung aufgefordert werden.
- **Manueller Proxy:** Diese Option wird benötigt, wenn Sie eine SSH-Tunnelverbindung zu Ihrem E-Mail-Server verwenden oder wenn der Computer, auf dem PGP Desktop ausgeführt wird, gleichzeitig als E-Mail-Server dient.

Hinweis: Wenn Sie einen manuellen Proxy verwenden und mehrere Messaging-Dienste nutzen, vergewissern Sie sich, dass die vom Messaging-Dienst verwendeten Umleitungsports eindeutig sind. Standardmäßig verwendet PGP Desktop die Ports 10143, 10110 und 10025 für alle Messaging-Dienste. Wenn Sie die Umleitungsports für einen Messaging-Dienst ändern möchten, klicken Sie auf **Einstellungen**. Ändern Sie das Protokoll in **IMAP** und ändern Sie dann die Einstellung für **Lokalen Port umleiten**.

Instant Messaging-Einstellungen

Wenn der Computer durch eine Netzwerk-Firewall geschützt wird, müssen Sie u. U. den Netzwerkport ändern, der von AIM für Instant Messaging-Sitzungen verwendet wird. Die meisten Benutzer müssen diese Einstellung nicht ändern.



- **Zielport ignorieren:** Aktivieren Sie dieses Kontrollkästchen, um den Port zu ändern, der von AIM für Instant Messaging-Sitzungen verwendet wird. Geben Sie einen Wert ein, der nicht dem Standardport (5190) entspricht. Erkundigen Sie sich beim Netzwerkadministrator, ob Sie die Einstellung ändern müssen und welcher Port in diesem Fall festgelegt werden muss.

Laufwerkseinstellungen

Der Bereich **Laufwerk** enthält Einstellungen für Laufwerke, die mit PGP Virtual Disk und PGP Shredder geschützt sind.

Einstellungen
Allgemein
Schlüssel
Hauptschlüssel
Messaging
Laufwerk
Benachrichtigungen
Erweitert
PGP-Laufwerk deaktivieren
Deaktivierung von PGP-Laufwerken zulassen, wenn Dateien geöffnet sind
Deaktivieren im Standbymodus
Standbymodus verhindern, wenn PGP-Laufwerke nicht deaktiviert werden können
Sicher löschen
PGP Shred überschreitet die Mindestvorschriften der Datenträgerrichtlinien des US-Verteidigungsministeriums, Norm 5220.22-M, bereits bei drei Durchgängen. Obwohl eine größere Anzahl von Durchgängen zulässig ist, sind für moderne Diskhardware höchstens zwei Durchgänge erforderlich.
Anzahl der Durchgänge: 3
Vor dem sicheren Löschen immer warnen

Hinweis: Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, sind diese Einstellungen möglicherweise bereits konfiguriert.

Im Bereich **Laufwerk** sind folgende Einstellungen verfügbar:

- **Deaktivierung von PGP-Laufwerken zulassen, wenn Dateien geöffnet sind:** In der Regel kann ein PGP Virtual Disk-Laufwerk nicht automatisch deaktiviert werden, wenn auf dem Laufwerk Dateien geöffnet sind. Wenn diese Option aktiviert ist, kann das Laufwerk auch mit geöffneten Dateien deaktiviert werden. Dieses Verfahren wird als erzwungene Deaktivierung bezeichnet.

  Warnung: Falls Sie die Deaktivierung eines PGP Virtual Disk-Laufwerks erzwingen, während Dateien geöffnet sind, könnten Daten verloren gehen.

- **Deaktivieren im Standbymodus:** Wenn diese Option ausgewählt ist, deaktiviert PGP Desktop automatisch alle aktivierten PGP Virtual Disk-Laufwerke, sobald der Computer in den Standbymodus wechselt.
  - **Standbymodus verhindern, wenn PGP-Laufwerke nicht deaktiviert werden können:** Diese Einstellung steht nur zur Verfügung, wenn die Option **Deaktivieren im Standbymodus** aktiviert ist. Durch diese Option wird verhindert, dass der Computer in den Standbymodus wechselt, wenn ein PGP Virtual Disk-Laufwerk nicht deaktiviert werden kann.
- **Anzahl der Durchgänge:** PGP Shredder entfernt die Dateien sicher, indem sie normal gelöscht werden. Dann wird der Speicherplatz, der zuvor von den soeben gelöschten Dateien belegt war, mit Nullen überschrieben.

Mit diesem Verfahren können Dateien in nur wenigen Durchgängen sehr sicher gelöscht werden. Daher sind standardmäßig **3** Durchgänge vorgesehen, die ein äußerst hohes Maß an Sicherheit bieten. Sie können die gewünschte Sicherheitsstufe jedoch noch steigern, indem Sie diese Einstellung Ihren Bedürfnissen entsprechend auf bis zu 49 Durchgänge erhöhen.

Beachten Sie dabei, dass die zusätzliche Sicherheit mit einem erhöhten Zeitaufwand für das sichere Löschen der Dateien verbunden ist. Der Zeitaufwand ist von mehreren Faktoren abhängig, insbesondere jedoch von der Geschwindigkeit des Prozessors.

Folgende Richtlinien werden für die Anzahl der Durchgänge empfohlen:

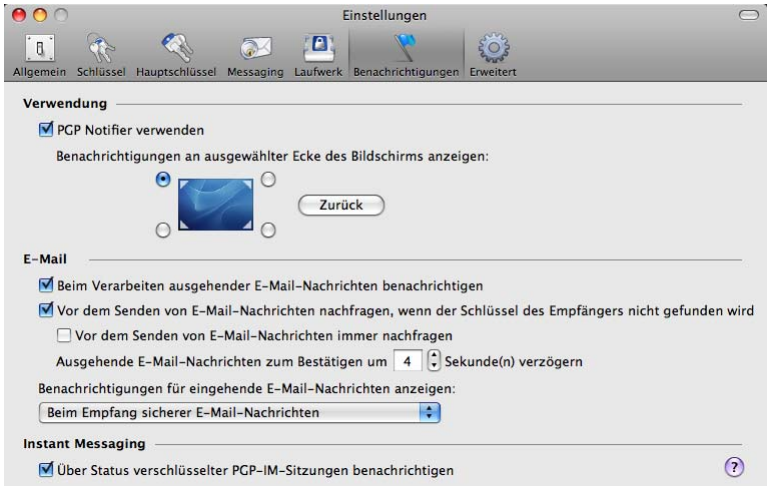
- 3 Durchgänge für den persönlichen Gebrauch
- 10 Durchgänge für den kommerziellen Gebrauch
- 18 Durchgänge für den militärischen Gebrauch
- 26 Durchgänge für maximale Sicherheit

- **Vor dem sicheren Löschen immer warnen:** Aktivieren Sie dieses Kontrollkästchen, wenn vor einem sicheren Löschvorgang stets ein Bestätigungsdialogfeld angezeigt werden soll. Dadurch können Sie nochmals überprüfen, ob wirklich nur die gewünschten Dateien sicher gelöscht werden. Diese Option ist standardmäßig aktiviert.

Benachrichtigungseinstellungen

Im Bereich **Benachrichtigungen** finden Sie Einstellungen für die Notifier-Funktion von PGP Desktop. Der Notifier zeigt Statusmeldungen in einer Ecke des Bildschirms an, wenn Sie E-Mail-Nachrichten senden oder empfangen. Darüber hinaus wird der Status angezeigt, wenn Sie die Laufwerksfunktionen von PGP Desktop verwenden.

In einer von einem PGP Universal Server verwalteten Umgebung hat der Administrator möglicherweise bestimmte Benachrichtigungseinstellungen festgelegt (z. B. die Anzeige von Benachrichtigungen oder die Position des Notifier-Fensters). In diesem Fall ist im Fenster „Einstellungen" der Bereich **Benachrichtigungen** nicht verfügbar und wird nicht angezeigt.



Im Bereich **Benachrichtigungen** sind folgende Einstellungen verfügbar:

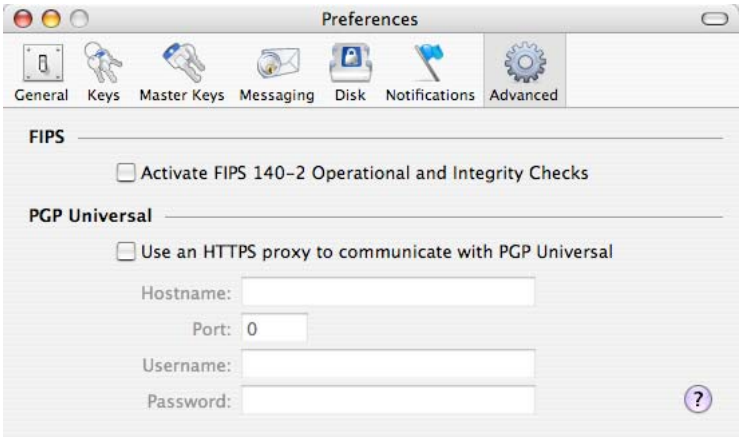
- **PGP Notifier verwenden:** PGP Desktop-Benachrichtigungen können in einer der vier Ecken des Bildschirms angezeigt werden. Wählen Sie mithilfe der entsprechenden Schaltfläche die Ecke aus, in der die PGP Desktop-Benachrichtigungen angezeigt werden sollen. Klicken Sie auf **Vorschau**, um zu testen, wie das PGP Desktop-Benachrichtigungsfenster in der betreffenden Ecke aussieht.
- **Beim Verarbeiten ausgehender E-Mail-Nachrichten benachrichtigen:** Aktivieren Sie dieses Kontrollkästchen, wenn beim Senden von E-Mail-Nachrichten Notifier-Meldungen von PGP Desktop mit Informationen zum Verschlüsselungs- und/oder Signierstatus angezeigt werden sollen. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie beim Senden von E-Mail-Nachrichten keine PGP Desktop-Benachrichtigungen wünschen.
- **Vor dem Senden von E-Mail-Nachrichten nachfragen, wenn der Schlüssel des Empfängers nicht gefunden wird:** PGP Desktop sucht nach einem öffentlichen Schlüssel für jeden Empfänger der von Ihnen gesendeten E-Mail-Nachrichten. Wenn für einen Empfänger kein öffentlicher Schlüssel gefunden werden kann, wird die betreffende E-Mail-Nachricht standardmäßig als Klartext (ohne Verschlüsselung) gesendet. Wenn Sie diese Benachrichtigungsoption von PGP Desktop auswählen, werden Sie in solchen Fällen benachrichtigt und erhalten die Möglichkeit, die betreffende E-Mail-Nachricht zu blockieren, damit sie nicht gesendet wird.

  Weitere Informationen zu den Einstellungen für die Standardrichtlinien von PGP Desktop finden Sie unter *Dienste und Richtlinien* (auf Seite 103).

- **Vor dem Senden von E-Mail-Nachrichten immer nachfragen:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie jede E-Mail-Nachricht vor dem Versand bestätigen möchten. Sie können den Verschlüsselungsstatus im Benachrichtigungsfenster von PGP Desktop überprüfen und dann entscheiden, ob die E-Mail-Nachricht gesendet oder blockiert werden soll.
- **Ausgehende E-Mail-Nachricht zum Bestätigen um n Sekunden verzögern** (wobei *n* für eine Zahl zwischen 1 und 30 steht; der Standardwert beträgt 4 Sekunden): Wählen Sie diese Option, wenn Sie für jede gesendete Nachricht eine PGP Desktop-Benachrichtigung erhalten möchten, jedoch nicht jedes Mal auf Ihre explizite Zustimmung gewartet werden soll. Ausgehende E-Mail-Nachrichten werden verzögert und eine Notifier-Meldung von PGP Desktop wird für die von Ihnen festgelegte Zeitdauer angezeigt. Wenn Sie möchten, dass die E-Mail-Nachricht gesendet wird, müssen Sie keine Maßnahmen ergreifen. Die E-Mail-Nachricht wird nach Ablauf der festgelegten Zeit gesendet. Wenn Sie die PGP Desktop-Benachrichtigung lesen möchten, zeigen Sie mit dem Mauszeiger darauf. Die PGP Desktop-Benachrichtigung wird dann nicht mehr transparent, sondern undurchsichtig angezeigt und die ausgehende E-Mail-Nachricht wird verzögert, während Sie die PGP Desktop-Benachrichtigung lesen. Anschließend können Sie entscheiden, ob die E-Mail-Nachricht gesendet oder blockiert werden soll.
- **Benachrichtigungen für eingehende E-Mail-Nachrichten anzeigen:** Geben Sie für eingehende E-Mail-Nachrichten an, in welchem Umfang Sie beim Empfang einer E-Mail-Nachricht über deren Status informiert werden möchten. Folgende Optionen sind verfügbar:
  - **Beim Empfang sicherer E-Mail-Nachrichten**: Beim Empfang sicherer E-Mail-Nachrichten wird ein PGP Desktop-Benachrichtigungsfenster angezeigt. Dieses Fenster enthält den Absender der E-Mail-Nachricht, den Betreff, den Verschlüsselungs- sowie den Verifizierungsstatus und die E-Mail-Adresse des Absenders.
  - **Nur beim Fehlschlagen der Nachrichtenüberprüfung**: Ein PGP Desktop-Benachrichtigungsfenster wird nur dann für eingehende E-Mail-Nachrichten angezeigt, wenn PGP Desktop die Signatur der eingehenden E-Mail-Nachricht nicht verifizieren kann.
  - **Nie**: Wählen Sie diese Option aus, wenn beim Empfang von E-Mail-Nachrichten kein PGP Desktop-Benachrichtigungsfenster angezeigt werden soll. Diese Option wirkt sich nicht auf PGP Desktop-Benachrichtigungen für ausgehende E-Mail-Nachrichten aus.
- **Über Status verschlüsselter PGP-IM-Sitzungen benachrichtigen**: Aktivieren Sie dieses Kontrollkästchen, wenn zu Beginn und bei Beendigung eines sicheren Instant Messaging-Chats kurz ein PGP Desktop-Benachrichtigungsfenster angezeigt werden soll.

Erweiterte Einstellungen

Die Einstellungen im Bereich **Erweitert** müssen von den meisten Benutzern nicht geändert werden.



Folgende erweiterte **Einstellungen stehen zur Verfügung:**

- **Funktions- und Integritätsprüfungen nach FIPS 140-2 aktivieren:** Wählen Sie diese Option aus, wenn von Ihnen oder von Ihrer Organisation Überprüfungen nach FIPS 140-2 durchgeführt werden sollen. Beachten Sie jedoch, dass die Computerleistung dadurch beeinträchtigt wird. Sie müssen den Computer neu starten, damit diese Einstellung übernommen wird. Diese Option steht nur bei eigenständigen Installationen zur Verfügung.
- **HTTPS-Proxy für Kommunikation mit PGP Universal verwenden:** Ändern Sie diese Einstellungen nur, wenn Sie vom Netzwerkadministrator dazu aufgefordert werden.

Wenn für Ihre Installation von PGP Universal Server eine sichere Client-Server-Verbindung über einen Proxy erforderlich ist, können Sie dies über diese Einstellungen angeben. Informationen zu Servername, verwendetem Kommunikationsport, Benutzer-ID und Kennwort zur ordnungsgemäßen Konfiguration dieses Abschnitts erhalten Sie vom Administrator.

A Mit Kennwörtern und Passphrasen arbeiten

Kennwörter und Passphrasen werden verwendet, um Informationen zu schützen. Passphrases, wörtlich übersetzt Schlüsselsätze, sind länger als Kennwörter und können mehrere Wörter und eine breitere Palette an Zeichen verwenden. Da der Ausdruck „Passphrase“ im Deutschen nicht sehr gebräuchlich oder verständlich ist, wird in diesem PGP-Produkt zum leichteren Verständnis der Ausdruck Passphrase verwendet. Sie können als Passphrase aber auch ganze Sätze verwenden. Sie erreichen dadurch eine höhere Sicherheit als mit einfachen Kennwörtern.

Ein Beispiel für ein einfaches Kennwort ist ein Wort mit vier Buchstaben oder zwei zusammenhängende Worte: „wennarbeit“ ohne die Anführungszeichen. Ein stärkeres Kennwort beinhaltet außerdem Großbuchstaben: WennArbeit. Noch besser ist es, wenn Sie Ziffern hinzufügen: Wenn9Arbeit4.

Im Vergleich hierzu sind Passphrasen länger und verwenden eine breitere Palette von Zeichen. Eine einfache Passphrase ist zum Beispiel: „Mb&iw>8aG.“ (ohne Anführungszeichen, aber mit Punkt). Diese Passphrase scheint zwar auf den ersten Blick schwer merkbar zu sein, da sie jedoch auf einem einfachen Satz basiert, lässt sie sich leichter merken.

Passphrasen können auch aus einfachen Sätzen bestehen, z. B. aus einem Buch, einschließlich der Satzzeichen und Groß-/Kleinschreibung. „Weil das nicht Golf ist, antwortete ich“ (einschließlich Anführungszeichen). Obwohl dies nicht nach einer starken Passphrase aussieht, ist es doppelt so stark wie die bisherigen Beispiele.

In diesem Abschnitt werden die Unterschiede zwischen Kennwörtern und Passphrasen beschrieben. Zudem finden Sie hier Informationen zur Passphrasen-Qualitätsanzeige in PGP Desktop sowie Richtlinien zum Erstellen starker Passphrasen.

In diesem Kapitel

Entscheidung über die Verwendung eines Kennwortes oder einer Passphrase 234
Die Passphrasen-Qualitätsanzeige 234
Starke Passphrasen erstellen 235
Vorgehensweise bei vergessenen Passphrasen 237
Passphrasen im Schlüsselanhänger speichern 238

Entscheidung über die Verwendung eines Kennwortes oder einer Passphrase

Wie entscheiden Sie, ob Sie ein Kennwort oder eine Passphrase verwenden sollten? Das hängt davon ab, was Sie schützen möchten. Je wertvoller die Informationen sind, die Sie schützen möchten, desto stärker sollte der Schutz sein.

Die meisten Word-Dokumente sind überhaupt nicht geschützt. Ihr Inhalt ist nicht wichtig genug, damit der Aufwand gerechtfertigt ist. Für Ihr Online-Banking benötigen Sie bereits mindestens eine vierstellige PIN. Abhängig von Ihrem Kontostand stellt das ein sehr hohes oder sehr niedriges Sicherheitsniveau dar. Für Ihre unwichtige Korrespondenz verwenden Sie vielleicht ein Hotmail-Konto. Ein einfaches Kennwort ist hierfür ausreichend. Für das E-Mail-Konto an Ihrem Arbeitsplatz, über das Sie interne Produkt-, Kunden- und Buchhaltungsinformationen erhalten, sollten Sie ein starkes Kennwort verwenden.

Mit PGP Desktop können Sie beispielsweise eine Passphrase für Ihr PGP-Schlüsselpaar und für Ihre PGP Virtual Disk-Laufwerke erstellen. Wenn Sie für Ihr PGP-Schlüsselpaar nur eine schwache Passphrase verwenden und ein Angreifer physischen Zugriff auf die private Schlüsseldatei hat, muss er lediglich die Passphrase herausfinden, um die Nachrichten, die Sie senden und empfangen, lesen zu können.

Die Passphrasen-Qualitätsanzeige

Beim Erstellen von Passphrasen in PGP Desktop kann die Passphrasen-Qualitätsanzeige als allgemeiner Anhaltspunkt für die Stärke der erstellten Passphrase verwendet werden. Auf jeden Fall handelt es sich um einen besseren Anhaltspunkt als lediglich die Anzahl der Zeichen.

Je länger die Anzeige, desto stärker ist im Allgemeinen die Passphrase. Was bedeutet die Länge der Passphrasen-Qualitätsanzeige jedoch wirklich?

Die Passphrasen-Qualitätsanzeige vergleicht die Zufallsmenge (Entropiewert) der von Ihnen eingegebenen Passphrase mit einer echten zufälligen Zeichenkette mit 128 Bit (was dem Entropiewert eines AES-128-Schlüssels entspricht). Dies wird als Entropie von 128 Bit bezeichnet.

(Entropie ist ein Maßstab für den Schwierigkeitsgrad beim Festlegen eines Kennworts oder eines Schlüssels.)

Wenn die von Ihnen erstellte Passphrase die Passphrasen-Qualitätsanzeige ungefähr halb ausfüllt, verfügt diese Passphrase über eine Entropie von etwa 64 Bit. Wenn die Passphrase die Passphrasen-Qualitätsanzeige komplett ausfüllt, weist diese Passphrase einen Entropie von etwa 128 Bit auf.

Wie stark ist demnach eine Entropie von 128 Bit? Ende der 90er Jahre wurden spezialisierte „DES-Cracker"-Computer gebaut, die innerhalb weniger Stunden durch Ausprobieren aller möglichen Schlüsselwerte einen DES-Schlüssel herausfinden konnten.

Wenn Sie einen Computer bauen könnten, der innerhalb einer Sekunde einen DES-Schlüssel herausfinden kann (der Computer müsste in der Lage sein, 255 Schlüssel pro Sekunde auszuprobieren), würde der Computer ca. 149 Billionen (Tausend Milliarden) Jahre benötigen, um einen AES-Schlüssel von 128 Bit herauszufinden. Im Vergleich dazu soll das Universum nicht einmal 20 Milliarden Jahre alt sein.

Wie wird die Entropie eines bestimmten Zeichens gemessen? Je größer die Menge von Zeichen ist, aus dem ein bestimmtes Zeichen ausgewählt werden kann, desto mehr Entropie wird dem ausgewählten Zeichen zugewiesen.

Wenn Sie beispielsweise eine numerische PIN auswählen sollen, beschränkt sich die Auswahl auf die Zahlen Null bis Neun, also insgesamt 10 Zeichen. Die Menge ist also recht klein und die Entropie für das ausgewählte Zeichen ist relativ gering.

Wenn Sie eine Passphrase mithilfe der englischen Version von PGP Desktop auswählen, ist die Sachlage jedoch anders. Sie können aus drei Mengen von Zeichen auswählen: Großbuchstaben und Kleinbuchstaben (52 Zeichen), den Zahlen Null bis Neun (10 Zeichen) und den Interpunktionszeichen auf einer Standardtastatur (32 Zeichen).

PGP Desktop bestimmt beim Eingeben eines Zeichens den Entropiewert für das jeweilige Zeichen basierend auf der Menge von Zeichen, der es angehört. Dieser Wert wird auf die Passphrasen-Qualitätsanzeige angewendet.

Das gleiche Konzept gilt für die Zeichensätze anderer Sprachen. Je größer die Datenbasis, desto mehr Entropie pro Zeichen. Wenn Sie z. B. einen asiatischen oder arabischen Zeichensatz verwenden, von denen manche über mehrere Hundert Zeichen verfügen, wäre die Entropie für ein ausgewähltes Zeichen entsprechend höher und die Passphrasen-Qualitätsanzeige würde wesentlich schneller ausgefüllt.

Starke Passphrasen erstellen

Beim Erstellen einer guten Passphrase wird in der Regel ein Kompromiss zwischen Benutzerfreundlichkeit und Stärke der Passphrase eingegangen. Längere Passphrasen mit Groß- und Kleinbuchstaben, Zahlen sowie Interpunktionszeichen sind zwar stärker, jedoch auch schwieriger zu merken.

Untersuchungen haben gezeigt, dass schwieriger zu merkende Passphrasen häufiger aufgeschrieben werden, was jedoch den Sinn einer starken Passphrase verfehlt. Es ist daher besser, eine kürzere starke Passphrase zu verwenden, die Sie sich merken können, als eine längere starke Passphrase, die Sie sich aufschreiben, um sie nicht zu vergessen.

Oft wird beim Erstellen von starken Passphrasen ein Ausdruck zu einzelnen Zeichen verkürzt. Als Beispiel wird folgender Ausdruck herangezogen:

```
Mein Bruder und ich wollen größere Acht aufeinander
geben.
```

Daraus ergibt sich folgende Passphrase:

```
Mb&iw>8aG.
```

Diese Passphrase besteht aus 10 Zeichen und enthält Groß- und Kleinbuchstaben, Zahlen sowie Interpunktionszeichen. Mit 10 Zeichen handelt es sich hierbei um eine relativ kurze Passphrase. Wenn 10 Zeichen Ihrer Meinung nach nicht ausreichen, können Sie entweder mit derselben Methode eine weitere Passphrase erstellen und dann beide zusammen verwenden oder einfach mit einem längeren Ausdruck beginnen.

Bei einer anderen Methode werden einfache Ausdrücke mit Interpunktionszeichen und Großbuchstaben verwendet. Beispiel:

```
Editiert von John Doe (nicht John Doe, Editor)
```

Hierbei handelt es sich um eine starke Passphrase, obwohl sie nicht besonders lang oder kompliziert ist. Wenn Sie einen Ausdruck aus einem Ihnen bekannten Buch verwenden, dürfen Sie das Buch nicht verlieren.

Sie können beim Erstellen einer Passphrase in PGP Desktop bis zu 255 Zeichen, einschließlich Leerzeichen, verwenden.

Ein weiterer Ansatz ist das Verknüpfen vieler kurzer, gängiger Wörter. Bei einer als Diceware™ bezeichneten Methode werden Würfel verwendet, um aus einer besonderen Liste, der Diceware Word List, die 7776 kurze englische Wörter, Abkürzungen und leicht zu merkende Zeichenketten enthält, zufällige Wörter auszuwählen. Wenn Sie eine ausreichende Anzahl dieser Zeichenketten zusammenfügen, können Sie eine starke Passphrase erstellen. In den häufig gestellten Fragen von Diceware wird angegeben, dass mit einer Passphrase aus 10 Diceware-Wörtern Entropie von 128 Bit erzielt werden kann.

Weitere Informationen zu Diceware finden Sie auf der *Diceware Passphrase-Website* (*http://world.std.com/~reinhold/diceware.html*).

Beachten Sie bei der Erstellung von Passphrasen Folgendes:

- Verwenden Sie eine Passphrase aus Ihrem Langzeitgedächtnis. Dadurch reduzieren Sie die Gefahr, dass Sie sie vergessen.
- Achten Sie darauf, dass die Passphrase mindestens acht Zeichen umfasst. Obwohl die Länge nicht mit der Stärke gleichzusetzen ist, ist eine lange Passphrase besser als eine kurze.
- Verwenden Sie Groß- und Kleinbuchstaben, Zahlen sowie Interpunktionszeichen.

Achtung: Verwenden Sie nach Möglichkeit nur ASCII-Zeichen. Dies ist besonders wichtig, wenn Sie internationale Tastaturen verwenden, da bestimmte Sonderzeichen (z. B. §) in Passphrasen nicht unterstützt werden.

- Ändern Sie die Passphrase regelmäßig, beispielsweise alle drei Monate. Je länger Sie dieselbe Passphrase verwenden, desto mehr Zeit geben Sie anderen, diese ausfindig zu machen.

Folgendes sollten Sie beim Erstellen von Passphrasen **vermeiden**:

- Schreiben Sie Ihre Passphrase nicht auf.
- Verraten Sie Ihre Passphrase niemals anderen Personen.
- Lassen Sie sich beim Eingeben der Passphrase nicht beobachten.
- Verwenden Sie nicht die Begriffe „Passwort“, „Kennwort“ oder „Passphrase“.
- Verwenden Sie keine Muster. Also nicht „abcdefgh“ oder „12345678“ oder „qwertzui“ oder „88888888“ oder „AAAAAAAA“.
- Verwenden Sie keine gebräuchlichen Wörter. Fast alle Hacker mit Erfahrung verwenden ein Wörterbuch zum Knacken von Kennwörtern, bei dem geläufige Wörter versucht werden. Verketten Sie nicht zwei gebräuchliche Wörter, verwenden Sie nicht die Pluralform eines geläufigen Wortes und verwenden Sie kein geläufiges Wort mit einem großen Anfangsbuchstaben.
- Verwenden Sie keine Zahlen, die sich auf Sie beziehen. Wenn jemand diese Zahlen kennt, könnten Hacker sie ausfindig machen. Verwenden Sie auf keinen Fall Ihr Geburtsdatum, Ihre Telefonnummer, Ihre Sozialversicherungsnummer oder Ihre Hausnummer.
- Verwenden Sie keine Namen. Verwenden Sie nicht die Namen von Personen, fiktiven Personen oder den Namen Ihres Haustiers. Verwenden Sie nicht den Namen Ihres letzten Urlaubsorts, Ihren Anmeldenamen oder den Namen Ihres Unternehmens. Verwenden Sie nicht den Namen Ihrer Lieblingsmannschaft oder eines Körperteils. Verwenden Sie außerdem keine Namen aus Büchern, insbesondere aus der Bibel.
- Verwenden Sie keine der oben genannten Wörter von hinten nach vorne gelesen oder mit einem einzelnen voran- bzw. nachgestellten Zeichen.

Vorgehensweise bei vergessenen Passphrasen

Wenn Sie Ihre Passphrase vergessen, können Sie Informationen, die an Ihren Schlüssel verschlüsselt wurden, nie mehr entschlüsseln. Sie können den Schlüssel jedoch wiederherstellen, wenn der PGP-Administrator eine Richtlinie zur Schlüsselwiederherstellung für Ihr Unternehmen implementiert hat. Weitere Informationen finden Sie unter *PGP-Schlüsselwiederherstellung* (siehe "*Schlüssel mit PGP Universal Server wiederherstellen*" auf Seite 90, "*Vorgehensweise bei verloren gegangenen Schlüsseln oder Passphrasen*" auf Seite 89). Sie können sich auch an den PGP-Administrator wenden.

Passphrasen im Schlüsselanhänger speichern

Bei Bedarf können Sie Schlüsselpassphrasen im Mac OS X-Schlüsselanhänger zwischenspeichern. Wenn Sie zur Eingabe einer Passphrase aufgefordert werden, aktivieren Sie das Kontrollkästchen **Passphrase im Schlüsselbund speichern**. Sie können dann auf alle Funktionen von PGP Desktop zugreifen, ohne die Passphrase jedes Mal eingeben zu müssen.

Unterschlüssel werden ebenfalls im Mac OS X-Schlüsselanhänger gespeichert. Die Aktionen der Unterschlüssel erfolgen also automatisch, wenn der Schlüsselanhänger entsperrt wurde.

B PGP Desktop mit PGP Universal Server verwenden

Mit PGP Universal Server können Unternehmen E-Mail-Nachrichten anhand konfigurierbarer Richtlinien, die vom PGP-Administrator zur Durchsetzung der Sicherheitsrichtlinien der Organisation erstellt werden, automatisch und (für den Endbenutzer) transparent geschützt werden. PGP Universal ermöglicht PGP-Administratoren darüber hinaus die Verwaltung der Bereitstellung von PGP Desktop an Benutzer innerhalb ihrer Organisation. Weitere Informationen zum PGP Universal Server finden Sie auf der Seite zum *PGP Universal Server auf der PGP-Website* (*http://www.pgp.com/products/universal/index.html*).

Wenn Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen, profitieren Sie bis zur Desktop-Ebene von der bewährten PGP-Verschlüsselungstechnologie sowie der weiteren Sicherheitsfunktionen in PGP Desktop, u. a. PGP Whole Disk Encryption, PGP Virtual Disk-Laufwerken, PGP Zip-Archiven und PGP Shredder.

Damit Sie PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung einsetzen können, müssen Sie PGP Desktop mithilfe eines vom PGP-Administrator erhältlichen Installationsprogramms installieren.

Wenn Sie eine Version von PGP Desktop für den privaten Gebrauch erworben haben und sie nicht in einem Unternehmensumfeld verwenden, haben Sie wahrscheinlich eine eigenständige Version, sodass dieser Abschnitt für Sie nicht relevant ist.

Achtung: Wenn Sie PGP Desktop in einem Unternehmensumfeld verwenden und das Installationsprogramm für PGP Desktop nicht vom PGP-Administrator erhalten haben, wenden Sie sich an den PGP-Administrator, **bevor** Sie diese Version von PGP Desktop installieren oder verwenden.

In diesem Abschnitt werden die Unterschiede bei der Verwendung von PGP Desktop in einer von einem PGP Universal Server verwalteten E-Mail-Domäne beschrieben.

In diesem Kapitel

Übersicht 240
Für PGP-Administratoren 241
Manuelle Bindung an einen PGP Universal Server 242

Übersicht

Das Installationsprogramm von PGP Desktop wurde vom PGP-Administrator auf eine der folgenden Weisen konfiguriert:

- **Keine Richtlinieneinstellungen**: Ihre Kopie von PGP Desktop verfügt nicht über integrierte Einstellungen. Sie können alle Funktionen verwenden, die von der Lizenz unterstützt werden.
- **Automatische Erkennung von Richtlinieneinstellungen**: Ihre Kopie von PGP Desktop wird eine Verbindung zu dem PGP Universal Server herstellen, der das Installationsprogramm erstellt hat, und wird die entsprechenden Einstellungen herunterladen. Aufgrund der erhaltenen Einstellungen müssen Sie Funktionen von PGP Desktop möglicherweise auf eine bestimmte Art und Weise verwenden.
- **Voreingestellte Richtlinieneinstellungen**: Die entsprechenden Einstellungen sind bereits in Ihre Kopie von PGP Desktop integriert. Aufgrund dieser Einstellungen müssen Sie Funktionen von PGP Desktop möglicherweise auf eine bestimmte Art und Weise verwenden.

Da Ihre Kopie von PGP Desktop Einstellungen von einem PGP Universal Server erhält, müssen Sie Funktionen von PGP Desktop möglicherweise auf eine bestimmte Art und Weise verwenden. Dies umfasst Folgendes:

- Möglicherweise müssen Sie bei der Installation von PGP Desktop bestimmte Aktionen ausführen. Es ist beispielsweise möglich, dass Sie das Startlaufwerk mit PGP Whole Disk verschlüsseln oder ein PGP Virtual Disk-Laufwerk erstellen müssen.
- Möglicherweise können oder müssen Sie Funktionen von PGP Desktop auf eine bestimmte Art und Weise verwenden. Eventuell müssen Sie Ihre Instant Messaging-Sitzungen mit AIM verschlüsseln oder Sie können Dateien beim Löschen automatisch sicher löschen.
- Möglicherweise können Sie bestimmte Funktionen von PGP Desktop nicht verwenden. Beispielsweise werden Sie ggf. daran gehindert, konventionelle Verschlüsselung zu verwenden oder selbstentschlüsselnde Archive (SDAs) zu erstellen.
- Möglicherweise müssen Sie bestimmte Messaging-Richtlinien einhalten. Beispielsweise kann es sein, dass Sie Nachrichten an bestimmte E-Mail-Domänen verschlüsseln und signieren müssen.
- Möglicherweise sind bestimmte Funktionen wie PGP Messaging oder PGP NetShare (unter Windows) deaktiviert oder Ihnen wird ein benutzerdefinierter PGP Whole Disk Encryption BootGuard-Bildschirm (unter Windows) angezeigt. Weitere Informationen finden Sie unter *Vom PGP Universal Server-Administrator angepasste Funktionen* (auf Seite 4).

Auf Funktionen von PGP Desktop, die von einem PGP-Administrator in einer von einem PGP Universal Server verwalteten Umgebung verwaltet werden können, wird in ihrer Beschreibung im gesamten Benutzerhandbuch hingewiesen.

Wenden Sie sich an den PGP-Administrator, um weitere Informationen zu den Unterschieden bei der Verwendung von PGP Desktop in einer von einem PGP Universal Server verwalteten Umgebung zu erhalten.

Für PGP-Administratoren

Falls Sie als PGP-Administrator die Implementierung von PGP Desktop für manche oder alle Benutzer in Ihrer Organisation verwalten, empfiehlt die PGP Corporation, den PGP Desktop-Benutzern die Verwaltung ihrer eigenen Schlüssel zu überlassen. Dies geschieht mithilfe des Client Key Mode.

Bei der Vorbereitung zur Erstellung der Installationsprogramme von PGP Desktop auf dem PGP Universal Server können Sie bestimmen, ob die PGP Desktop-Benutzer die Möglichkeit erhalten, ihre eigenen Schlüssel zu verwalten (Client Key Mode) oder ob der PGP Universal Server die Schlüsselverwaltung für die Benutzer übernimmt (Server Key Mode).

Diese Einstellungen werden bei der Schlüsseleinrichtung im Standardbildschirm im Bereich für die Schlüsselverwaltung festgelegt, der Teil der Konfiguration der standardmäßigen Benutzergruppenrichtlinie für interne Benutzer ist (**Benutzergruppe > Richtlinienoptionen > Schlüsseleinrichtung: Standard** in der Administrator-Oberfläche des PGP Universal Servers).

Für PGP Desktop-Benutzer ist der Client Key Mode aus folgenden Gründen die bessere Wahl:

- Viele PGP Desktop-Funktionen erfordern, dass die Benutzer ihre privaten Schlüssel verwalten. Wenn diese Schlüssel vom PGP Universal Server verwaltet werden, sind die entsprechenden Funktionen für die PGP Desktop-Benutzer nicht zugänglich.
- Im Server Key Mode sind bestimmte Optionen nicht verfügbar, die Sie für die PGP Desktop-Benutzer vorkonfigurieren. Beispielsweise ist die automatische Erstellung von PGP Virtual Disk-Laufwerken nicht möglich.

Manuelle Bindung an einen PGP Universal Server

Bei der manuellen Bindung an einen PGP Universal Server mit PGP Desktop (klicken Sie beim Anzeigen eines Messaging-Dienstes auf **Servereinstellungen**) und der Anmeldung laden Sie nur die E-Mail-Richtlinie und keine Consumer-Richtlinie herunter. Der PGP Universal Server-Administrator hat möglicherweise andere Optionen in der Consumer-Richtlinie festgelegt (z. B. Schlüsselmodi, Erzwingen der Verschlüsselung von Laufwerken usw.). Zur vollständigen Verwaltung und zum Erzwingen der Consumer-Richtlinie müssen Sie eine „gekennzeichnete“ Installation von PGP Universal Server verwenden. Wenden Sie sich an den Administrator, um bei Bedarf eine gekennzeichnete Installation zu erhalten.

Darüber hinaus ist bei der manuellen Bindung an einen PGP Universal Server die Datei `PGPtrustedcerts.asc` nicht unter C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\PGPCorporation\PGP vorhanden. Wenn Sie eine manuelle Bindung an einen PGP Universal Server durchführen möchten, müssen Sie diese Datei erstellen und sicherstellen, dass die Benutzer-ID des Organisationsschlüssels in dieser Datei dem durch PGPSTAMP angegebenen Server entspricht (Domänenname und IP-Adresse müssen übereinstimmen).

Index

.

.Mac, Schlüssel synchronisieren mit - 220

A

Adressenlisten-Richtlinien - 120, 121, 122
AES, Algorithmus in PGP Virtual Disk - 198
Allgemeine Einstellungen - 218
alternative Passphrasen - 166, 191
ändern
  Ihre Passphrase - 70
  Passphrase eines Schlüssels - 70
anmelden im PGP Bootguard-Bildschirm - 164
Anwendernamen, auf Schlüsseln - 68
ausgehende E-Mail-Nachrichten - 101
Authentifizierung für PGP Whole Disk Encryption
  verwendete Methode, festlegen - 158
Automatischer Modus - 226

B

Benutzer - 190
  PGP Whole Disk Encryption, hinzufügen oder löschen aus - 166, 167
Bewertungslizenzen - 5
Bindung, manuell an einen PGP Universal Server - 242
biometrische Wortliste - 66
BootGuard - See PGP BootGuard-Bildschirm

C

CAST, Algorithmus in PGP Virtual Disk - 198
Client-Schlüsselmodus (CKM) - 132

D

Dateien
  öffentliche Schlüssel exportieren - 59
  öffentliche Schlüssel importieren aus - 66
Dateien sicher löschen - See sicheres Löschen von freiem Speicherplatz
Daten von einem verschlüsselten Laufwerk wiederherstellen - 172
Dauerlizenzen - 5
deaktivieren - 206
  PGP Portable-Laufwerke - 206
  PGP Virtual Disk-Datenträger - 187
deinstallieren - 25, 170
designierter Widerrufer - 84
Dienste - 103
  aktivieren - 108
  anzeigen - 104
  deaktivieren - 108
  erstellen - 105
  löschen - 108
Dienste, Messaging - 103, 109
Dienste-Menü
  PGP-Funktionen - 39
digitale Signatur löschen - 71
digitale Signaturen - 56, 57, 60, 71, 79, 94
Dock-Symbol - See PGP Dock-Symbol

E

eingehende E-Mail-Nachrichten - 98
Einstellungen - 147, 217
  Allgemein - 218
  Instant Messaging - 227
  Messaging - 223
  PGP Disk - 228
  PGP Viewer - 147
  Schlüssel - 220
Einzelplatzanwender - 3
E-Mail - 97
  Dienste und Richtlinien - 103
  exportieren
Schlüssel in Datei - 59
  in PGP Viewer öffnen - 145
  in Posteingang kopieren - 146
  mehrere Konten - 109
  Nachrichten in Posteingang exportieren - 146
  Notifier - 32
  öffentliche Schlüssel kopieren aus - 61
  öffentlichen Schlüssel anhängen - 58
  Schlüsselmodi - 132
  schützen - 97
E-Mail-Optionen - 226
Energiesparmodus, Mac OS X und PGP WDE - 177
entfernen

Foto-ID von einem Schlüssel - 66
Unterschlüssel - 82
Entourage 2004, Integration mit - 24
entschlüsseln und verifizieren
in Finder - 42
erstellen - 50, 235
Messaging-Dienst - 105
Messaging-Richtlinie - 112
neues PGP Virtual Disk-Laufwerk - 183
Passphrasen, starke - 235

F

Fehlerbehebung - 110
Finder, zugreifen aus - 32, 39
Fingerabdruck, digitalen verifizieren - 72
Flags für Verwendung, bei Unterschlüsseln - 81
Flags für Verwendung, festlegen - 81
Forensik, Datenwiederherstellung - 172
Foto-ID - 66
entfernen - 66
hinzufügen - 66
von einem Schlüssel entfernen - 66
Freien Speicherplatz sicher löschen - See sicheres Löschen von freiem Speicherplatz

G

geteilte Schlüssel wieder zusammenfügen - 86, 87
Grundbegriffe - 3, 11, 15, 103, 132
Grundlegende Schritte für die Verwendung - 16
Guarded Key Mode (GKM) - 132
Gültigkeit - 66

I

Ihre Passphrase ändern - 70
importieren
öffentliche Schlüssel, von Dateien - 66
PGP-Schlüssel in Finder - 44
IM-Sitzungen verschlüsseln - 97, 139, See PGP Messaging
installieren - 25
Instant Messaging - 139
Optionen - 227

K

Kennwörter - See Passphrasen
Keyserver - 13
durchsuchen - 60, 61
fremde öffentliche Schlüssel abrufen - 60, 61
öffentlichen Schlüssel senden an - 57
zur Verteilung widerrufener Schlüssel verwenden - 85
Keyserver durchsuchen - 60, 61
komprimieren, PGP Virtual Disk-Laufwerk - 189
konventionelle Verschlüsselung - 40

L

Laufwerk umschlüsseln - 168, 189
Laufwerke
Anwender zu verschlüsselten Laufwerken hinzufügen - 166
entfernbar - 175
Fehler während Verschlüsselung - 162
unterstützt in PGP WDE - 154
verschlüsseln - 158, 159
Verwendung, verschlüsselt - 163
Lese-/Schreibfehler - 158
Lese-/Schreibfehler bei Laufwerkverschlüsselung - 158
Lizenzierung - 5, 24, 153
lokale Richtlinie - See Offline-Richtlinie
löschen
Benutzer-IDs - 71
digitale Signaturen - 71
Schlüssel - 71
Schlüssel von Ihrem Schlüsselbund - 71
Unterschlüssel - 82

M

Mail-Server, siehe Messaging-Dienste - See Messaging
Markierungen, festgelegte Verwendung bei Unterschlüsseln - 81
mehrere Messaging-Services - 109
Menüleistensymbol - 29
Messaging - 103
Fehlerbehebung - 110
mehrere - 109
Notifier - 32
Messaging-Einstellungen - 223
Messaging-Protokoll - 136
Mietlizenzen - 5

N

NetShare - See PGP NetShare
Notifier-Funktion
  Beschreibung - 32
  für ausgehende Nachrichten - 34
  für eingehende Nachrichten - 34
  für Instant Messaging - 35

O

öffentliche Schlüssel - 13
  aktivieren und deaktivieren - 72
  an andere Personen verteilen - 56
  an Keyserver senden - 57
  andere öffentliche Schlüssel abrufen - 60
  aus Dateien importieren - 66
  aus E-Mail-Nachrichten kopieren - 61
  E-Mail-Nachricht, anhängen an - 58
  in Datei exportieren - 59
  in Datei speichern - 59
  Keyserver durchsuchen - 60, 61
  signieren - 74
  verifizieren - 72, 73
  vertrauen - 77
  von einem Keyserver abrufen - 61
  Vorteile des Versands an einen Keyserver - 57
öffentliche Schlüssel aktivieren - 72
öffentliche Schlüssel deaktivieren - 72
Offline-Richtlinie - 35, 101, 102, 104
Optionen - See Einstellungen

P

Partitionen, verschlüsseln - 166
Passphrase
  alternative Passphrasen für PGP Virtual Disk hinzufügen - 166
  ändern - 70
  ändern auf einem Schlüssel - 70
  in Schlüsselbund speichern - 238
  vergessen - 237
Passphrasen - 199, 233
  ändern - 70, 168, 205
  stark, erstellen - 235
  unterstützte Zeichen in PGP WDE - 159
  vergessen - 89, 90
Passphrasen-Qualitätsanzeige - 234
Passphrase-Qualitätsanzeige - 234
PGP BootGuard-Bildschirm - 159, 164
PGP Desktop
  Beschreibung - 11
  deinstallieren - 25
  Einrichtungsassistent - 24
  Hauptbildschirm - 27, 28
  in einer von PGP Universal verwalteten Umgebung - 240
  Installation - 19
  installieren - 19
  Notifier-Funktion - 32
  PGP-Symbol in der Taskleiste - 29
  Richtlinienbeschreibung - 103
  SSL/TLS-Support - 130
  Symbol in der Menüleiste - 29
  Systemvoraussetzungen - 19
  Upgrade durchführen - 21
  zugreifen über Finder - 32
PGP Desktop auf einen anderen Computer übertragen - 25
PGP Desktop installieren - 19
PGP Disk
  Einstellungen - 228
PGP Dock-Symbol - 30
PGP Global Directory - 11
PGP Keys - See Schlüssel
  anzeigen - 48
  importieren in Finder - 44
  Schlüsseleinstellungen im Expertenmodus - 52
  Schlüsselpaar erstellen - 50
  zu Schlüsselbund hinzufügen in Finder - 45
PGP Messaging - 11, 97
  Dienst erstellen - 105
  Dienste und Richtlinien - 103
  Dienstebeschreibung - 103
  Protokoll - 136
  Richtlinie erstellen - 112
PGP NetShare - 11
PGP Shredder - 11, 213
  Beschreibung - 213
PGP Universal - 4, 90, 239
PGP Universal Server - 11, 90, 170, 239, 241, 242
PGP Universal-Dienstprotokoll (USP) - 62
PGP Viewer - 143, 145, 146, 147, 148

E-Mail-Nachrichten - 145, 146
Übersicht über - 143
PGP Virtual Disk - 11, 181, 199
aktivieren - 187
aktivieren in Finder - 43
alternative Benutzer - 191
Austauschen - 197
deaktivieren - 187
Eigenschaften - 186
erstellen - 183
Laufwerk aktivieren in Finder - 43
löschen - 195
neues Laufwerk erstellen - 183
pflegen - 195
Sicherheitsmaßnahmen - 199
Sichern - 196
umschlüsseln - 189
Verschlüsselungsalgorithmen - 198
PGP Virtual Disk-Laufwerke aktivieren - 187
PGP Whole Disk Encryption - 11
Authentifizierungsoptionen - 158
automatische Sicherungssoftware - 169
Benutzer hinzufügen - 166
Benutzer löschen - 167
Benutzern, arbeiten mit - 166, 167, 168
deinstallieren - 170
Laufwerk verschlüsseln - 158
Laufwerk vorbereiten für - 153
Laufwerk, PGP WDE-verschlüsseltes verwenden - 163
Laufwerk, Schutz aufrechterhalten vom - 165
Laufwerkstypen, unterstützte - 154
Lese-/Schreibfehler - 158
Lizenzierung - 153
Passphrase ändern - 168
PGP Universal Server, verwaltet - 170
Schlüsselinformationen anzeigen - 166
Sicherheitsmaßnahmen - 176
umschlüsseln - 168
unterstützte Laufwerkstypen - 154
verschlüsseltes Laufwerk entschlüsseln - 174
verschlüsseltes Laufwerk umschlüsseln - 168
Verschlüsselung vorbereiten - 153
Verschlüsselungsdauer, berechnen - 157
Wechseldatenträger - 175
Wiederherstellungs-CD - 173
Wiederherstellungs-Token - 171
PGP Zip - 11, 207
PGP Zip-Archive
Beschreibung - 207
erstellen - 208
extrahieren in Finder - 45
öffnen - 210
verifizieren signierter - 210
Verifizierungsverlauf löschen - 210
PGP Zip-Archive in Finder extrahieren - 45
PGP-Administrator - 170, 239, 240
PGP-Keyserver-Liste - See Keyserver
PGP-Protokoll - 136
Platzhalter, in Richtlinien - 118
primärer Name auf dem Schlüssel - 68
private Schlüssel - 13, 54
Protokoll, Messaging - 136

R

Richtlinie aktualisieren - 102
Richtlinien - 103
anzeigen - 104
bearbeiten - 123
Beispiele - 112
Beispiele für Messaging - 120
erstellen - 112
löschen - 129
Messaging erstellen - 112
Standardrichtlinien - See Standardrichtlinien
Ruhezustand - See Energiesparmodus, Mac OS X und PGP WDE

S

S/MIME-E-Mail-Nachrichten, Zertifikate importieren - 69
Schlüssel - 47, 65

aktivieren - 72
aus dem Schlüsselbund löschen - 71
deaktivieren - 72
Einstellungen - 220
E-Mail, anhängen an - 58
E-Mail-Adressen, hinzufügen zu - 68
exportieren - 59
Finder, hinzufügen in - 45
Foto-ID ersetzen - 66
geteilten Schlüssel wieder zusammenfügen - 86, 87
Größe festlegen von - 80
Keyserver, hochladen auf - 58
mehrere Anwendernamen und E-Mail-Adressen - 68
Namen, hinzufügen zu - 68
öffentliche Schlüssel in Datei speichern - 59
öffentliche Schlüssel verifizieren - 72
Passphrase ändern - 70
schützen - 94
signieren - 74
synchronisieren, Schlüsseleinstellungen - 220
teilen - 86
Unterschlüssel - 77
verloren - 89, 90
vertelen, öffentlicher - 56
Vertrauen für Validierungen gewähren - 76, 77
widerrufen - 84, 85
wiederherstellen - 90
Schlüssel oder Passphrase verloren - 89
Schlüssel schützen - 94
Schlüssel teilen - 86
Schlüssel validieren - 76
Vertrauen gewähren für - 77
Schlüssel wiederherstellen - 56, 90
Schlüsselbund, Passphrase speichern in - 238
Schlüsselbunde - 54, 71
Schlüsselgröße
Ausgleich - 80
festlegen - 80
Schlüsselmodi - 132
Schlüsselmodus zurücksetzen - 132
Schlüsselpaar - 13
Schlüssel-Wiederherstellung - 24, 90, See Schlüssel wiederherstellen
separater Signatur-Unterschlüssel - 11
Server Client Key Mode (SCKM) - 132
Server-Schlüsselmodus (Server Key Mode, SKM) - 132
sicher löschen
Beschreibung - 213
in Finder - 42
Sichere Instant Messaging-Anwendung (IM) - 139
sicheres Löschen von freiem Speicherplatz - 11
Sicherheitsmaßnahmen - 176, 199
Signaturen, aus Schlüsseln löschen - 71
signieren - 71
in Finder - 40
öffentliche Schlüssel - 74
Schlüssel - 71, 74
Smartcard - 13
SSL/TLS-Support - 130
Standardrichtlinien - 103, 120, 121, 122
starke Passphrasen - 235
Startlaufwerke, verschlüsseln - 152, 178
Support, Kontaktaufnahme - 8, 9
Systemvoraussetzungen - 19

T

Tastatur, in PGP WDE unterstützt - 155
technischer Support - 9
technischer Support, Kontaktaufnahme - 8
Textausgabe - 40
Twofish, Algorithmus in PGP Virtual Disk - 198

U

Übersicht, über PGP Desktop - 1
umschlüsseln - 168
Universal Server - See PGP Universal
Unterschlüssel - 77
Ablaufdatum - 77, 80
ansehen - 79
anzeigen - 77
arbeiten mit - 77
Eigenschaften - 77
entfernen - 82
Größe - 77
Größe festlegen von - 80
Gültigkeit - 77
neu erstellen - 80
separat - 77
Symbole - 77
widerrufen - 82
Unterschlüssel anzeigen - 77

Unterschlüssel-Verwendung - 81
Upgrade durchführen - 23
USP - See PGP Universal-Dienstprotokoll (USP)

V

vergessene Passphrasen - 90
verifizieren
  öffentlicher Schlüssel - 73
  signierte PGP Zip-Archive - 210
Verifizierungsverlauf löschen - 210
verschlüsseln
  in Finder - 40
verschlüsseln und signieren
  in Finder - 40
Verschlüsselung
  Anwender aus PGP WDE löschen - 167
  Anwender hinzufügen - 166
  Dauer berechnen in PGP WDE - 157
  Laufwerk oder Partition umschlüsseln - 168
  Laufwerke oder Partitionen - 159
  Laufwerksfehler während - 162
  PGP WDE-verschlüsselte Laufwerke verwenden - 170
  Pilottest - 157
  verwendeter Algorithmus - 198
Verschlüsselungsoptionen
  konventionell - 40
  MacBinary - 40
  Original sicher löschen - 40
  Textausgabe - 40
vertrauen
  für Schlüsselvalidierungen gewähren - 77
  öffentliche Schlüssel - 77
Vertrauen für Schlüsselvalidierungen gewähren - 77
Vertrauen gewähren - 76
Vertrauen, für Schlüsselvalidierungen gewähren - 76
Virtual Disk-Laufwerke verteilen - 197
virtuelle Laufwerke - See PGP Virtual Disk
virtuelle Laufwerke austauschen - 197

W

Wechseldatenträger - 175
Wechseldatenträger in PGP WDE - 175
widerrufen
  Schlüssel - 85
  Signatur, von einem Schlüssel - 76
  Unterschlüssel - 82
Widerrufer, Schlüssel - 84
Wiederherstellungs-Token - 171
Wortliste, biometrische - 66

X

X.509-Zertifikate - 69
X.509-Zertifikate, zu Schlüsselpaar hinzufügen - 70

Z

Zeichen, in PGP WDE unterstützt - 159
zentral verwaltete Anwender - 3
Zusätzliche Verschlüsselungsschlüssel (Additional Decryption Keys, ADK) - 82